MESTRADO EM DIREITO E CIÊNCIA JURÍDICA

ESPECIALIDADE - DIREITOS FUNDAMENTAIS

A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL E OS *DARK PATTERNS* NAS REDES SOCIAIS: UMA ANÁLISE SOBRE A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

THAÍS FIGUEIRA DE OLIVEIRA

LISBOA

2023

THAÍS FIGUEIRA DE OLIVEIRA
62045

A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL E OS *DARK PATTERNS* NAS REDES SOCIAIS: UMA ANÁLISE SOBRE A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Dissertação apresentada como exigência parcial à obtenção do título de Mestre em Direito e Ciência Jurídica ao Curso de Mestrado em Direito e Ciência Jurídica, na Especialidade de Direitos Fundamentais da Faculdade de Direito da Universidade de Lisboa, sob a orientação do Senhor Professor Doutor Domingos Miguel Soares Farinho.

LISBOA
2023

Aos meus queridos e amados mamãe e papai.

Tudo por eles e para eles.

Sempre.

AGRADECIMENTOS

Em meio a uma pandemia decidi que era a hora de trilhar novos rumos em busca de qualificação profissional e amadurecimento pessoal. Saí então do conforto da casa dos meus pais e atravessei o oceano para experimentar novas experiências, desafios e até mesmo algumas dificuldades. Reconheço que fui forte e consegui vencer cada uma das fases e questões que me foram apresentadas. No entanto, sei que não trilhei todo este caminho até aqui sozinha, pois tive o apoio e a participação de pessoas muito especiais. O percurso do mestrado contou com a ajuda de muitas pessoas importantes e eu terei gratidão por toda a vida por tudo o que recebi de cada uma, como o apoio, as palavras de afeto e incentivo, os conselhos e a companhia.

Ao professor dr. Domingos Farinho, meu professor orientador, por todos os ensinamentos que recebi desde a disciplina de Direito Constitucional, a qual sem dúvida teve grande contribuição para minha transição de carreira para a área do Direito Digital, até esta fase da escrita da dissertação. Ao professor dr. Jorge Miranda, com quem tive a honra de estudar Direitos Fundamentais, e ao professor dr. Pedro Lomba, com quem escolhi estudar Justiça Constitucional e aprendi a gostar do tema da proteção de dados pessoais. Ao professor dr. Pierluigi Perri, meu orientador no intercâmbio ERASMUS na Università degli Studi di Milano, pela recepção mais que especial e por todos os ensinamentos transmitidos sobre a inteligência artificial.

Aos meus colegas do curso de mestrado, pelas recomendações de materiais, pelo apoio e pela companhia nas horas de estudo. À FDUL como um todo, por proporcionar encontros e eventos que enriqueceram meus conhecimentos e ser o local onde pude compartilhar ideias e conhecer pessoas que foram fundamentais para a conclusão do curso.

À minha família, meus avós, meus tios e tias, primos e primas, pois sei que mesmo de longe, todos estão na torcida pelo meu sucesso e crescimento.

Aos meus amigos de Manaus, minha cidade natal, os quais mesmo à distância estiveram presentes e contribuíram de alguma forma para a conclusão desta fase. Dentre todos aqueles que carrego com muito carinho, agradeço em especial à Evellin Souza, por ser mais que amiga, a minha irmã de coração.

Aos amigos de Lisboa, por fazerem desta cidade a nossa casa e por serem a família que estou construindo aqui. Dentre todas as pessoas a quem agradeço por estarem comigo em cada etapa vivida, por quem continua aqui e por quem esteve mas tomou outros rumos, em especial agradeço à Tereza Cunha e à Tatiana Malafaia, por terem sido, cada uma em uma fase diferente, minhas amigas para o lazer e minhas companhias para o estudo na biblioteca.

Ao meu companheiro de vida Gabriel Valença, por sempre estar comigo, tanto nas horas de lazer como naquelas dedicadas ao estudo, aconselhando-me quando necessário e ajudando-me sempre que possível.

E aos meus pais, Julieta e José Roberto, por serem tudo o que se espera de uma mãe e de um pai: amigos, conselheiros, professores e incentivadores. Meu eterno agradecimento por tudo o que sempre foi feito por mim e para mim, inclusive o próprio patrocínio deste curso, já que não obtive bolsa nem qualquer outra ajuda. Sem dúvida esta é a realização de um sonho para todos nós e este título será, como tudo, por vocês e para vocês.

“As pessoas nunca controlam realmente o seu comportamento, mesmo quando pensam que o controlam.” DWORKIN, Ronald.

RESUMO

Os *dark patterns* são entendidos como técnicas de manipulação presentes de forma obscura e subliminar nos sistemas de inteligência artificial que compõem a interface de usuário das plataformas de redes sociais, com a finalidade de arbitrariamente provocar a distorção da consciência das pessoas e, em consequência, influenciar e alterar seus comportamentos. Através de diferentes recursos inseridos no *design*, buscam subverter a autonomia dos usuários, ao interferir em suas escolhas e no exercício de seus direitos. Esta investigação analisa a problemática dos *dark patterns* inseridos na arquitetura digital das redes sociais para verificar quais mecanismos legais já existentes podem servir à resolução de tal questão, se as propostas legislativas de regulação da inteligência artificial podem ser medidas suficientes ou mesmo se seria necessário elaborar um novo documento legal para esse fim. Observou-se que nos sistemas legais analisados, quais sejam, União Europeia, Brasil e Estados Unidos da América, não se dispõe até o momento de uma lei especialmente concebida para enfrentar e proibir tais práticas em sua totalidade. Há documentos legais sobre temáticas do direito digital que podem ter alguma aplicação para a questão dos *dark patterns*, assim como as propostas de regulação da inteligência artificial podem ser um meio para tratar o assunto. Além disso, há a possibilidade de interpretações extensivas de leis de proteção de dados pessoais e de direito dos consumidores, bem como de resolver o evidente conflito entre direitos fundamentais por meio da interpretação constitucional, a fim de realizar uma concordância prática entre os direitos envolvidos. Desta forma, a regulação da inteligência artificial apresenta-se como medida necessária não somente para possibilitar a inovação e o desenvolvimento científico à luz de princípios éticos e morais, como também para assegurar a justa proteção aos direitos fundamentais no ambiente digital.

PALAVRAS-CHAVE: *dark patterns*; redes sociais; direitos fundamentais; regulação; inteligência artificial.

ABSTRACT

Dark patterns are defined as manipulation techniques applied in obscure and subliminal ways in artificial intelligence systems that form the user interface of social media platforms, with the aim of arbitrarily distorting people's consciousness and, as a result, influencing and changing their behavior. Through different design features, they attempt to subvert users' autonomy by interfering in their choices and the exercise of their rights. This research analyzes the problem of dark patterns inserted into the digital architecture of social media in order to assess what existing legal mechanisms can be used to address this issue, whether legislative proposals to regulate artificial intelligence can be sufficient as measures, or whether it would be necessary to draft a new legal document for this purpose. It was concluded that in the legal systems analyzed, which are the European Union, Brazil, and the United States of America, there is currently no law that specifically addresses and prohibits such practices. There are legal documents on digital law that are somewhat applicable to the issue of dark patterns, and the proposals for regulating artificial intelligence could provide a tool to address the issue. Furthermore, there is the possibility of interpreting other laws such as personal data protection and consumer laws extensively, as well as solving the conflict between fundamental rights through constitutional interpretation, to achieve a practical concordance between the rights involved. Therefore, the regulation of artificial intelligence is a necessary measure not only to promote innovation and scientific development based on ethical and moral principles but also to ensure fair protection of fundamental rights in the digital environment.

KEYWORDS: dark patterns; social media; fundamental rights; regulation; artificial intelligence.

NOTA DE ADVERTÊNCIA

A presente dissertação de mestrado foi escrita na Língua Portuguesa segundo seu uso no Brasil, conforme as normas do Novo Acordo Ortográfico da Língua Portuguesa.

Para a formatação, estilo e citação foram seguidas as diretrizes da Associação Brasileira de Normas Técnicas – ABNT.

LISTA DE SIGLAS E ABREVIATURAS

abr.	Abril
ago.	Agosto
AI	*Artificial Intelligence*
atual.	Atualizado
CRFB/1988	Constituição da República Federativa do Brasil
ed., eds.	Edição, edições; editora, editoras
et al.	*et alii*
EU	*European Union*
EUA	Estados Unidos da América
FTC	*Federal Trade Commission*
fev.	Fevereiro
IA	Inteligência Artificial
jan.	Janeiro
jun.	Junho
jul.	Julho
LGPD	Lei Geral de Proteção de Dados
mai.	Maio
mar.	Março
n.	Número
nov.	Novembro
org.	Organizador, organizadores
OECD	*Organization for Economic Co-operation and Development*
p.	Página.
reimp.	Reimpressão
rev.	Revisão, revista
s. d.	Sem data
s. l.	Sem local
set.	Setembro
Trad.	Tradução
UE	União Europeia
v.	Volume

SUMÁRIO

1 INTRODUÇÃO

Em uma sociedade progressivamente mais digital e conectada, o estilo de vida contemporâneo, para além de muitas atividades, tem sofrido sensíveis mudanças pelo emprego de sistemas dotados de inteligência artificial, com as mais diferentes funcionalidades. Essas transformações, as quais encaminharam-nos para a concepção atual de sociedade da informação[1], apontam para uma linha cada vez mais tênue entre o mundo virtual e o analógico. Assim, torna-se mais difícil separar a vida *online* da vida *offline*, visto que o tempo, o espaço, as interações sociais e as informações apresentam-se em uma relação cada vez mais conectada. O desenvolvimento acentuado e o aprimoramento dessas ferramentas, aliados a múltiplas possibilidades de aplicação, têm levado ao seu crescente e intenso uso, desde em situações cotidianas até para as finalidades mais complexas.

Reconhecendo que a virtualidade revela-se como uma nova dimensão da realidade[2], os sistemas de IA vêm tornando-se cada dia mais importantes e, em alguns casos, até mesmo indispensáveis. No entanto, embora a IA traga vastos e inegáveis proveitos em muitos contextos nos quais é aplicada atualmente, levanta também uma série de questões em seu desenvolvimento, implementação e utilização, como a evidência de riscos a direitos fundamentais, conflitos éticos e morais, dentre outros problemas.

Desde o lançamento dos blogs pessoais, dos primeiros sites de bate-papo virtual e das primeiras redes sociais, o mundo passou a experimentar uma inédita forma de manifestar e exercer diversos direitos fundamentais, como a privacidade, a imagem e as liberdades de expressão, comunicação e informação. Espaços privados mas de uso público transformaram-se em grandes praças públicas digitais nas quais as pessoas comunicam-se, relacionam-se, expõem detalhes de suas vidas privadas, compartilham opiniões e até comercializam bens e serviços, dentre diversas outras possibilidades de uso.

A maior parte dos serviços e funcionalidades nas redes sociais é disponibilizada gratuitamente, isto é, sem custos ao usuário. Isso porque o principal produto de negócio desse tipo de empresas é justamente a informação, dentre as quais as relativas aos seus usuários têm um alto valor de mercado. Assim, para coletar mais dados pessoais, é necessário oferecer um ambiente atraente e interessante para que as pessoas sintam-se livres e motivadas a passarem mais tempo conectadas e, com isso, compartilhá-los. Para isso, a arquitetura digital das redes

---

[1] FLORIDI, Luciano. **Information: A Very Short Introduction**. New York: Oxford University Press, 2010.
[2] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Editora Foco, 2022. p. 1.

sociais passou a ser minunciosamente elaborada para, por intermédio de sistemas de IA e da defraudação do *design* de suas interfaces de usuário, serem capazes de não somente recolher tais informações, mas influenciar o comportamento das pessoas e suas decisões.

Por meio da aplicação dos *dark patterns*, os quais constituem sistemas de IA concebidos para promover a distorção da consciência das pessoas a fim de alterar seus comportamentos, as redes sociais exercem um poder de controle sobre seus usuários, visto que comandam a oferta de opções, a disposição de informações e a exibição de publicações e publicidade, dando maior preferência àquelas que correspondem aos seus próprios interesses e conveniências. Assim, não é o usuário quem personaliza como será sua rede pessoal através de suas escolhas e preferências, é a própria rede social quem manipula o usuário de acordo com seus interesses de negócio. Por intermédio da tecnologia dos sistemas de IA são elaborados diversos tipos de padrões obscuros com diferentes finalidades ocultas, as quais podem ser levar as pessoas a desembolsar mais dinheiro, fornecer mais dados pessoais e a gastar mais tempo de atenção conectadas à plataforma, consumindo o conteúdo essencialmente direcionado a elas.

Frente a essas novas formas de violações e riscos aos direitos fundamentais, imprescindível faz-se a chamada à ciência jurídica para garantir a devida tutela aos bens jurídicos envolvidos. Desta forma, a presente investigação propõe-se a analisar a problemática dos *dark patterns* inseridos no contexto das redes sociais para verificar quais mecanismos legais já existentes podem servir à resolução de tal questão, se as propostas legislativas que objetivam regular a inteligência artificial apresentam-se como medidas suficientes ou mesmo se seria necessário elaborar um novo documento legal para essa finalidade.

Assim, para atingir o objetivo determinado, seguiu-se uma metodologia de pesquisa descritiva, por meio da coleta de dados e informações de diferentes fontes científicas, tais como artigos científicos, livros e doutrinas tanto de Direito como de outras áreas, tendo em vista a transdisciplinaridade do tema da inteligência artificial. Ademais, foi feito o exame das normas legais já consolidadas e de projetos de lei em andamento em três diferentes ordenamentos jurídicos, quais sejam, a União Europeia, o Brasil e os Estados Unidos, a fim de verificar se haveria uma harmonia entre os referidos sistemas legais no enfrentamento do problema e na proteção dos direitos fundamentais. Além disso, utilizou-se o método indutivo para, a partir das observações apontadas, elaborar conclusões acerca da resolução do problema de pesquisa destacado.

Justifica-se a ênfase sobre os mencionados ordenamentos jurídicos, quais sejam, a União Europeia, o Brasil e os Estados Unidos da América, na medida em que o referido bloco europeu tem buscado manter uma posição de vanguarda no tratamento de temas relacionados

ao Direito Digital, visto que, tal como realizado com seu regulamento para a proteção de dados pessoais, tenta novamente construir um documento regulatório que possa impactar positivamente outros sistemas legais. Não obstante, escolheu-se examinar o Brasil tendo em vista a sua importância representada em termos econômicos, sociais, jurídicos e políticos não apenas para a região da América Latina, mas também para os países considerados em desenvolvimento. Por sua vez, demonstra-se a pertinência em inserir os EUA em tal debate considerando que as maiores empresas de tecnologia, de IA e de redes sociais têm sedes nesse país. Assim, busca-se apresentar o tratamento do tema e suas diferentes abordagens nos sistemas destacados.

Em vista disso, no capítulo 2, a fim de compreender a temática, inicialmente discorrer-se-á sobre a inteligência artificial em uma contextualização, passando por uma breve análise de seu percurso histórico-evolutivo. Ademais, serão examinadas as questões acerca de sua conceituação de uma forma geral, tendo em vista que a sua característica pluridisciplinar carrega divergências para a sua compreensão. Ainda, comentar-se-ão algumas de suas definições legais propostas em documentos regulatórios, uma vez que para que a sua regulação seja eficaz, entende-se que a abordagem realizada não pode ser restrita demais, de modo a prejudicar a futura inclusão de novos sistemas e tecnologias, nem tão abrangente, pelo que comprometa a própria efetividade da lei.

Em sequência, no capítulo 3 será apresentada a questão dos *dark patterns*, sua relação com os sistemas de IA, bem como uma compreensão conceitual do tema. Explica-se que, embora existam várias nomenclaturas para identificar tais técnicas, escolheu-se utilizar o referido termo em razão de ainda ser o mais conhecido atualmente. Posteriormente, será comentado brevemente o seu desenvolvimento histórico, de modo a esclarecer de que forma e por qual razão tais padrões passaram a serem utilizados nas interfaces digitais, sobretudo nas redes sociais, as quais correspondem ao foco da presente pesquisa. Não obstante, serão relacionadas em uma classificação as diferentes espécies encontradas nesse mencionado ambiente virtual, organizados ao final em uma tabela na qual são destacados cada tipo, com uma sucinta descrição, identificação de seu objetivo e um exemplo de aplicação em uma rede social.

Por sua vez, no capítulo 4 comentar-se-ão algumas questões decorrentes da aplicação dos *dark patterns* nas interfaces de usuário nas redes sociais, especialmente aqueles desenvolvidos com a finalidade de manter o usuário conectado à plataforma pelo máximo de tempo possível. Assim, analisar-se-á a linha tênue entre a personalização do conteúdo e a manipulação do usuário, bem como a relação estabelecida com os padrões obscuros e o

profiling realizado por meio da coleta de dados pessoais. Além disso, serão mencionadas as interferências ocasionadas pelo uso de tais ferramentas no exercício e proteção de alguns direitos e liberdades fundamentais nesses espaços digitais de interação social.

No capítulo 5 apresentar-se-ão os mecanismos legais pelos quais o Direito pode intervir para fornecer a tutela necessária aos bens jurídicos envolvidos no problema exposto dos *dark patterns* nas redes sociais. Assim, discorrer-se-á acerca da resolução de conflitos entre os direitos fundamentais implicados, bem como sobre a legislação já existente nos ordenamentos jurídicos destacados e se representam meios suficientes para proporcionar a solução adequada a essas novas formas de violação a direitos. Além disso, serão comentados os projetos de regulação da inteligência artificial apresentados até o presente momento nesses sistemas legais e se serão medidas eficazes ao combate de tais técnicas e aptas à proteção dos referidos direitos das pessoas. E por fim, nas considerações finais comentar-se-ão as conclusões obtidas após a realização da presente investigação, bem como serão indicadas as lacunas existentes na academia que podem servir de objeto para futuras pesquisas.

2 A INTELIGÊNCIA ARTIFICIAL: UMA CONTEXTUALIZAÇÃO

Por meio de diferentes técnicas e envolvendo habilidades como associação, compreensão, planejamento, linguagem e coordenação motora, em tese a inteligência artificial tenta executar atividades próprias da mente humana[3]. Desde o seu surgimento, tem sido elaborada com diferentes objetivos, como desenvolver programas computacionais capazes de manifestar inteligência utilizando processos parecidos com os humanos, além de criar programas inteligentes que sejam capazes de complementar ou suplementar a inteligência humana em determinados trabalhos[4], assim como aplicar conceitos e modelos na busca por respostas a indagações relativas aos seres humanos e outros seres vivos[5].

O desenvolvimento do tema da IA iniciou-se por volta da década de 1950, sendo, inclusive, considerado como uma espécie de "rebelião" contra as ciências já existentes e suas limitações, como a estatística e a teoria de controle, do campo da engenharia[6]. Sua origem se deu por meio de estudos acadêmicos transdisciplinares que envolveram diversas ciências, sobretudo os campos da robótica, matemática e da ciência da computação, bem como foi impulsionada através de livros do gênero de ficção científica[7]. Isso porque as histórias desse gênero suscitavam desde questionamentos a reflexões críticas[8], além de que serviam como inspiração para a delimitação dos limites éticos da nova área em expansão[9].

Autores como Isaac Asimov abordavam em suas histórias a interação entre humanos e criaturas robóticas com inteligência. Tratavam de cenários sociais, quase sempre distópicos, relacionados com teorias científicas e a evolução da tecnologia, como por exemplo a criação de robôs dotados de inteligência que, ao alcançarem um estado de perfeição, eram capazes de governar o mundo segundo seus próprios interesses. No bojo de suas histórias, Asimov

---

[3] BODEN, Margareth A. **Mind as machine: a history of cognitive science**. v. 1. Oxford: Oxford University Press, 2006. p. 4.

[4] SIMON, Herbert A. **Artificial intelligence: an empirical science**. Artificial Intelligence. v. 77, n. 1, p. 95–127, 1995. Disponível em: <https://www.sciencedirect.com/science/article/pii/000437029500039H?ref=cra_js_challenge&fr=RR-1> Acesso em jan. 2023.

[5] BODEN, Margareth A. **AI: its nature and future**. Oxford: Oxford University Press, 2016. p. 2.

[6] RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022. p. 43.

[7] HAENLEIN, Michael; KAPLAN, Andreas. **A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence**. California: California Management Review, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0008125619864925?casa_token=zVeExM_jERMAAAAA:LFj7BHbmorHWyYWpZmDm5DcTSJL900kV450sAMUa7UsC821NRBVD-P7OxkK_F3H1SdWd3SLVDEjtLA> Acesso em jan. 2023. p. 2.

[8] LEE, Kai-fu. QIUFAN, Chen. **Inteligência Artificial 2041: Dez Visões para o Nosso Futuro**. Trad. Maria do Carmo Figueira. Lisboa: Relógio D'Água, 2023. p. 23.

[9] HIDALGO, César A. **How Humans judge Machines**. Cambridge, Massachusetts: The MIT Press, 2021. p. 2.

mencionou enunciados que, conquanto não detivessem força normativa, viriam a ser considerados como as primeiras leis da robótica, evidenciando assim a influência da literatura na referida área[10].

Seguindo pelo campo dos estudos acadêmicos, cientistas começaram a explorar a viabilidade matemática da criação artificial de inteligência. Dentre os acontecimentos mais significativos que introduziram a trajetória histórico-evolutiva da área, merecem destaque os primeiros resultados promissores atribuídos ao matemático britânico Alan Turing e a Conferência de Dartmouth, dos professores Marvin Minsky e John McCarthy.

No ano de 1950, Alan Turing apresentou o estudo pioneiro *"Computing Machinery and Intelligence"* sobre como criar máquinas inteligentes e testar sua inteligência, pelo qual buscava responder à questão se máquinas poderiam pensar[11]. O teste, proposto por Turing como *The Imitation Game*, mas que ficou conhecido como *Turing Test*, ainda hoje é reconhecido por parte dos pesquisadores de IA como um modelo, não para testar se um sistema funciona de forma inteligente, mas se ele pode se comportar como um humano. Basicamente, consiste em verificar se um humano, ao interagir com outro humano e uma máquina, não é capaz de distingui-los[12].

Embora Turing tenha reformulado suas investigações posteriormente[13], o *Turing Test* também foi criticado e considerado controverso e irrealista por outros pesquisadores, além de reputar-se que pode ter prejudicado os avanços da IA, tendo em vista que seus pressupostos são meramente comportamentais. Ademais, o tipo de comportamento linguístico requerido no teste é geralmente relacionado como o cerne da cognição humana. Portanto, dever-se-ia avaliar

---

[10] As reconhecidas Três Leis da Robótica criadas por Isaac Asimov em seu livro "Eu, robô" (1950), determinam que (i) um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano venha a ser ferido, (ii) um robô deve obedecer às ordens dadas por seres humanos, exceto nos casos em que tais ordens entrem em conflito com a Primeira Lei e (iii) um robô deve proteger sua própria existência, desde que tal proteção não entre em conflito com a Primeira ou com a Segunda Lei. Mais tarde, Asimov adicionou outro enunciado, considerado como "Lei Zero", pois seria anterior às demais. Segundo esta, um robô não pode fazer mal à humanidade e, nem por omissão, permitir que ela sofra algum mal. ASIMOV, Isaac. **Eu, robô**. Trad. Aline Storto Pereira. - São Paulo: Aleph, 2015. Disponível em: <https://ia801503.us.archive.org/17/items/Livros-isaac-asimov/Eu%2C Robo - Isaac Asimov.pdf> Acesso em nov. 2022.

[11] TURING, Alan M. **Computing Machinery and Intelligence**. Mind, vol. LIX/236, 1950. p. 433-460. Disponível em: <https://academic.oup.com/mind/article/LIX/236/433/986238> Acesso em fev. 2023.

[12] HAENLEIN, Michael; KAPLAN, Andreas. **A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence**. California: California Management Review, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0008125619864925?casa_token=zVeExM_jERMAAAAA:LFj7BHbmorHWyYWpZmDm5DcTSJL900kV450sAMUa7UsC821NRBVD-P7OxkK_F3H1SdWd3SLVDEjtLA> Acesso em jan. 2023. p. 2.

[13] LACERDA, Bruno Torquato Zampier**. Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 21.

também como o mecanismo alcança a inteligência e levar em consideração a organização interna de seu sistema[14].

Responder à simples questão se máquinas poderiam pensar pode não ser tão simples assim, devido aos diferentes entendimentos que podem ser extraídos acerca dos significados das palavras empregadas, quais sejam, máquinas, o ato de pensar e o que se entende por poder[15]. Por isso, critica-se que, em vez de proporem respostas a essa pergunta, os cientistas de IA não buscam aprofundar o complexo processo do pensamento humano, mas apenas verificam quais ferramentas foram desenvolvidas em uma máquina e atribuem a isso terminologias humanas[16].

Ainda na década de 1950 foi realizado o *Dartmouth Summer Research Project on Artificial Intelligence*, conferência histórica organizada pelos professores Marvin Minsky e John McCarthy, dentre outros como Allen Newell e Herbert Simon, nos Estados Unidos. Na ocasião, diversos pesquisadores de várias áreas reuniram-se para discutir a possibilidade de produção de IA, por meio da construção de máquinas capazes de simular aspectos relacionados à aprendizagem e à inteligência humana. Embora a conferência à época não tenha tido as contribuições que seus organizadores esperavam, ainda assim é considerada um marco no desenvolvimento das pesquisas nesse setor, além de ter sido a primeira vez em que o termo *artificial intelligence* foi utilizado na academia como uma disciplina de estudo[17].

O percurso de evolução da temática ao longo dos anos apresenta momentos de altos e baixos[18], isto é, períodos de entusiasmo com investimentos elevados em investigação acadêmica, com a apresentação de significativos avanços tecnológicos, chamados de *AI Spring*, bem como outros com mais ceticismo com redução de orçamentos, devido ao pouco interesse por pesquisas na área, chamados de *AI Winter*[19]. Isso porque, entre as décadas de 1970 e 1980, a área experimentou uma escassez de dados, considerados fundamentais para seu

---

[14] ARKOUDAS, Konstantine; BRINGSJORD, Selmer. **Philosophical Foundations**. In: FRANKISH, Keith; RAMSEY, William M. The Cambridge Handbook of Artificial Intelligence. Cambridge: Cambridge University Press, 2014. Disponível em: <https://www.cambridge.org/core/books/the-cambridge-handbook-of-artificial-intelligence/3DCB2E04739722A99EDE86B7A34A30E3> Acesso em mai. 2023. p. 35.

[15] NILSSON, Nils J. **Artificial Intelligence: A New Synthesis**. Morgan Kaufmann Publishers, 1998. p. 2.

[16] PESSIS-PASTERNAK, Guitta. **Será Preciso Queimar Descartes? Do caos à inteligência artificial: quando os cientistas se interrogam**. Trad. de Manuel Alberto. – Lisboa: Relógio D'Água, 1993. p. 197.

[17] MOOR, James. **The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years**. AI Magazine, vol. 27, n. 4, 2006. Disponível em: <https://aaai.org/ojs/index.php/aimagazine/article/view/1911/1809> Acesso em mar. 2023.

[18] Diferente da maioria dos doutrinadores, Coelho (1995) propõe uma descrição da evolução da IA em analogia aos períodos históricos. Assim, os anos de 1956 a 1960 seriam a pré-história, de 1960 a 1965 a alvorada, de 1965 a 1970 a idade negra, de 1970 a 1975 o renascimento, de 1975 a 1985 os anos de ouro e de 1985 a 1995 seria a idade ecológica (considerando a data de publicação do referido livro). COELHO, Helder. **Inteligência Artificial em 25 lições**. Fundação Calouste Gulbenkian, 1995. p. 23.

[19] GRUDIN, Jonathan. **AI and HCI: Two Fields Divided by a Common Focus**. AI Magazine, *[S. l.]*, v. 30, n. 4, p. 48, 2009. DOI: 10.1609/aimag.v30i4.2271. Disponível em: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2271> Acesso em abr. 2023.

desenvolvimento, aliada à capacidade reduzida de processamento dos recursos computacionais disponíveis à época[20].

Essa oscilação entre a diminuição do financiamento e o aumento da descrença com relação ao potencial de satisfação de seus objetivos inovadores, com questionamentos acerca da possibilidade do real alcance de inteligência em sistemas e computadores pode ser entendida como consequência do *AI Effect*. Costuma-se argumentar que, ao compreender a tecnologia no processo de um dito sistema com IA, diz-se que ele não apresenta uma inteligência real, ou seja, é como se a inovação tecnológica perdesse a sua "magia"[21].

Em entendimento mais recente, afirma-se que esse dito efeito se manifesta como mecanismo psicológico de defesa humana ao verificar os avanços tecnológicos oferecidos pela IA e seus atributos, muitas vezes parecidos aos humanos, pelo que as pessoas tendem a ver as características humanas como mais distintas e essenciais[22]. Aliada a esse efeito, pode-se também observar a chamada "lei de Amara", pela qual percebem-se críticas a uma tendência em curto prazo à superestimação de uma tecnologia enquanto, por outro lado, uma subestimação a longo prazo[23], tendo em vista que as expectativas das pessoas com relação às tecnologias mudam conforme seu aprimoramento e uso[24].

Entre primaveras promissoras com significativos progressos científicos, mas também invernos com descobertas limitadas[25], a IA avançou ao longo dos anos, relacionando-se a

---

[20] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Editora Foco, 2022. p. 22.

[21] HAENLEIN, Michael; KAPLAN, Andreas. **A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence**. California: California Management Review, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0008125619864925?casa_token=zVeExM_jERMAAAAA:LFj7BHbmorHWyYWpZmDm5DcTSJL900kV450sAMUa7UsC821NRBVD-P7OxkK_F3H1SdWd3SLVDEjtLA> Acesso em jan. 2023. p. 2.

[22] SANTORO, Erik; MONIN, Benoît. **The AI Effect: People rate distinctively human attributes as more essential to being human after learning about artificial intelligence advances**. Journal of Experimental Social Psychology, vol. 107, n. 104464, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0022103123000215?pes=vor> Acesso em mai. 2023.

[23] LEE, Kai-fu. QIUFAN, Chen. **Inteligência Artificial 2041: Dez Visões para o Nosso Futuro**. Trad. Maria do Carmo Figueira. Lisboa: Relógio D'Água, 2023. p. 19.

[24] FITZPATRICK, Noel; KELLEHER, John D. **On the Exactitude of Big Data: La Bêtise and Artificial Intelligence**. La Deluziana, 2018. doi: 10.21427/dfw8-m918. Disponível em: <https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1005&context=gradcamart> Acesso em jun. 2023. p. 5.

[25] Grande parte dos autores costumam referenciar os momentos históricos da inteligência artificial dividindo-os apenas entre *AI Spring* e *AI Winter*. Entretanto, Haenlein e Kaplan (2019) ampliam a análise histórico-evolutiva da disciplina adicionando o *AI Fall* e o *AI Summer*, em alusão às quatro estações. Segundo os autores, o *AI Spring* corresponderia à década de 1950 com o início do desenvolvimento de pesquisas na área, seguido pelo *AI Summer*, período subsequente à Conferência de Dartmouth de plena expansão e sucesso por duas décadas. Já o *AI Winter* representaria o hiato nas descobertas pelo agravamento do ceticismo, vivido em meados da década de 1970. E o *AI Fall* seria o período recente em que a IA pouco progrediu e apenas colheu os frutos das pesquisas e avanços estatísticos iniciados no passado, como o desenvolvimento de redes neurais artificiais. HAENLEIN, Michael; KAPLAN, Andreas. **A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence**. California: California Management Review, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0008125619864925?casa_token=zVeExM_jERMAAAAA:LFj7

fatores como a evolução da internet e o progresso da informática, na reconhecida terceira revolução industrial ou revolução digital. Essa expansão informática, proporcionou um aumento na capacidade de processamento de dados, aliado a uma enorme disponibilidade de todo tipo e formato de informações, o que potencializou a criação e o aprimoramento de diferentes sistemas dotados com IA[26], sobretudo das técnicas de *machine learning* e *deep learning*.

Esse conjunto de acontecimentos resulta no período presente de alto desenvolvimento tecnológico em diferentes frentes, bem como com a progressão da IA e sua relação com os domínios físicos, digitais e biológicos na chamada quarta revolução industrial[27]. Com reflexos em diferentes setores como o transporte, manufatura, saúde, educação e negócios, a IA tem imposto profundas mudanças na forma como o mundo funciona e em como a sociedade se organiza, tal como aconteceu com o advento da eletricidade mais de cem anos atrás[28].

Isto posto, nesta parte da pesquisa serão analisadas as questões acerca da conceituação da IA, visto que por ser um ramo da ciência abundante em pluralidade e transdisciplinaridade, enfrenta profundas divergências para sua compreensão. Do mesmo modo, ver-se-á a seguir que essa dificuldade se reflete também em sua definição legal, uma vez que para que sua regulação seja eficaz, seu espectro não pode ser nem tão restrito, para não limitar a inclusão e identificação de novas tecnologias a surgir, nem tão amplo que possa afetar sua própria efetividade.

2.1 A conceituação da IA e sua divergência

De maneira simples, a inteligência artificial pode ser entendida como algo similar à inteligência humana, sendo que os progressos na área podem ser indicados pelo grau de similaridade alcançada por sistemas e máquinas com relação aos humanos[29]. De forma um pouco mais detalhada, a IA corresponde atualmente a sistemas presentes em máquinas com

BHbmorHWyYWpZmDm5DcTSJL900kV450sAMUa7UsC821NRBVD-P7OxkK_F3H1SdWd3SLVDEjtLA> Acesso em jan. 2023.

[26] LEE, Kai-fu. **Inteligência artificial: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos**. Trad. de Marcelo Barbão. 1. ed. – Rio de Janeiro: Globo Livros, 2019. p. 19.

[27] SHWAB, Klaus. **The Fourth Industrial Revolution**. World Economic Forum, 2016. p. 11-15.

[28] LYNCH, Shana. **Andrew Ng: Why AI Is The New Electricity**. Insights by Stanford Business, 2017. Disponível em: <https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity> Acesso em mar. 2023.

[29] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 363.

capacidade de, através da análise de dados e o estabelecimento de objetivos e critérios, realizar tarefas simples ou complexas com determinado grau de autonomia e assim apresentar resultados. No entanto, elaborar uma definição que abarque todas as diferentes modalidades de IA sem que a limite, mas que também seja capaz de abranger o surgimento de novas tecnologias, nunca pareceu ser uma missão atingível, por qualquer ciência que se utilize como parâmetro.

Considerando que a própria inteligência transborda complexidade, pelo que até se considera não poder ser definida[30], árduo encargo igualmente se constitui não somente definir, mas compreender a inteligência artificial, juntamente com seus diferentes sistemas e representações. Uma temática transdisciplinar, que atravessa áreas como a informática, a estatística, a robótica, a matemática e a engenharia, como também perpassa por outras ciências, tais como a neurociência, a linguística, a filosofia, a sociologia, assim como o direito e a psicologia. Entender que a IA floresce bebendo em diferentes fontes científicas é parte fundamental de um processo que objetiva a sua regulação perante o direito, em vista de que esse ajuste legal não a limite, mas, pelo contrário, estimule seu desenvolvimento, implementação e utilização por toda a sociedade que dela se beneficia, ou por ela de algum modo é afetada.

Conforme mencionado anteriormente, o termo inteligência artificial começou a ser utilizado na ocasião da conferência de 1956 de Dartmouth e tem sua autoria atribuída aos professores Marvin Minsky e John McCarthy. Na conjuntura, no entanto, não foi conferido um significado nem explicação à expressão, mas apenas se referia a uma nova área de estudo que se pretendia investigar. A nomenclatura buscava abarcar a nova disciplina acadêmica, a qual se propunha basicamente a descobrir como fazer máquinas apresentarem atributos da inteligência humana, como utilizar linguagem, formar conceitos e abstrações e resolver problemas, até mesmo se auto aperfeiçoar e autocorrigir[31]. A expressão passou a ser utilizada após o referido evento e com a publicação do estudo *"Steps Towards Artificial Intelligence"*[32], de Minsky no ano de 1961, no qual se pretendia apontar as competências necessárias para o desenvolvimento de um sistema com IA, bem como traçar um possível caminho para o progresso da área[33].

---

[30] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 362.

[31] NILSSON, Nils J. **The Quest for Artificial Intelligence: a history of ideas and achievements**. Cambridge University Press, 2010.

[32] MINSKY, Marvin. **Steps Toward Artificial Intelligence**. IRE, 1960. Disponível em: <https://web.media.mit.edu/~minsky/papers/steps.html> Acesso em mar. 2023.

[33] SHIRAI, Yoshiaki; TSUJII, Jun-ichi. **Inteligência Artificial: conceitos, técnicas e aplicações**. Tradução de António Realinho. Publicações Europa América, 1988. p. 7.

Entretanto, até mesmo sobre a definição da nomenclatura houve discordância, tendo em vista que cada diferente nome proposto tentava identificar um tipo de projeto de investigação diferente na área. Assim, enquanto John McCarthy apresentava o termo *artificial intelligence* na conferência de 1956, outros estudiosos como Herbert Simon e Allen Newell defendiam a utilização da expressão "processamento de informação complexa", ou "simulação de processos cognitivos". Já para outros cientistas, a exemplo de Donald Michie, termos como "inteligência mecânica" ou "inteligência de máquinas" faziam mais sentido,[34] além de outros como *cognology* ou *heuristic programming*[35].

Devido à discordância quanto à nomenclatura da IA, a qual leva a uma indeterminação da acepção do termo e a críticas por apresentar questões de ordem semântica, alguns teóricos ainda sugerem atualmente a utilização alternativa do termo inteligência computacional, dentre outros possíveis nomes[36]. Contudo, dentre diferentes sugestões, a expressão inteligência artificial ganhou popularidade por força da ampla utilização em uma grande quantidade de livros, cursos acadêmicos, periódicos e conferências[37].

Considerando que a palavra artificial significa algo criado por ação humana, isto é, ausente de naturalidade, sua junção à palavra inteligência (sobre a qual não se entrará no debate acerca de suas definições, variações e interpretações) no termo IA pode trazer questões acerca do parâmetro para determinar se algo é dotado de inteligência artificial. Assim, a expressão por si só já carrega conflitos sobre se o critério para ser uma IA viria a ser equivalente à inteligência humana, diferente ou até mesmo superior[38].

Ao longo da história de seu desenvolvimento, diferentes significados foram outorgados ao termo, ao passo que os estudos na área e suas descobertas foram progredindo, bem como conforme diferentes versões de IA foram sendo criadas. Isso porque considera-se que não haveria um único objetivo determinado na área, mas que seu propósito muda com o tempo. Além disso, conforme seus diferentes avanços são apresentados, há quem entenda que uma determinada técnica dotada com IA, ao ser incorporada à prática, deixa de ser considerada parte da inteligência artificial,[39] em mais uma manifestação do já mencionado *AI Effect*, podendo ter reflexos no sentido do termo.

---

[34] COELHO, Helder. **Inteligência Artificial em 25 lições**. Fundação Calouste Gulbenkian, 1995. p. 23.
[35] NILSSON, Nils J. **Artificial Intelligence: A New Synthesis**. Morgan Kaufmann Publishers, 1998. p. 8.
[36] MAGRANI, Eduardo. **A internet das coisas**. – Rio de Janeiro: FGV Editora, 2018. p. 25.
[37] NILSSON, Nils J. **Artificial Intelligence: A New Synthesis**. Morgan Kaufmann Publishers, 1998. p. 8.
[38] CLARKE, Roger. **Why the world wants controls over Artificial Intelligence**. Computer Law and Security Review, v. 35, n. 4, p. 423–433, 2019. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919301268> Acesso em mar. 2023. p. 424.
[39] SHIRAI, Yoshiaki; TSUJII, Jun-ichi. **Inteligência Artificial: conceitos, técnicas e aplicações**. Tradução de António Realinho. Publicações Europa América, 1988. p. 9.

Parte das divergências sobre a conceituação dessa expressão deriva do fato de que alguns pesquisadores costumam relacionar o significado de inteligência do termo a aspectos humanos, até porque a própria ciência da IA busca reproduzir de forma artificial em modelos, sistemas e máquinas características relacionadas à inteligência humana. Deste modo, alguns assimilam seu sentido ao desempenho humano, enquanto outros associam à racionalidade humana e os processos internos de pensamento e raciocínio e, outros, a um comportamento humano inteligente como uma característica exterior. A partir disso, conectando esses quatro fatores, quais sejam, humano, racionalidade, pensamento e comportamento, em quatro diferentes combinações, são desenvolvidas distintas abordagens e tipos de IA relacionados a diferentes áreas do conhecimento[40].

Assim, há investigações que buscam a criação de uma inteligência semelhante à humana com sistemas que agem como humanos (*acting humanly*), com reflexos na psicologia. Como exemplo, citam-se técnicas de IA que tentam comunicar-se de maneira satisfatória em um idioma humano, como o *natural language processing*, assim como aprender para adaptar-se a novas circunstâncias e detectar diferentes padrões no *machine learning*, ou mesmo movimentar-se e manipular objetos no segmento da robótica[41].

Por outro lado, há pesquisas experimentais com uma abordagem de modelagem da ciência cognitiva e da neurociência que buscam observar o funcionamento do cérebro humano e, assim, serem capazes de "ler mentes" e desenvolver pensamentos tal como os humanos (*thinking humanly*). Além disso, há a junção da lógica da filosofia e da probabilidade da matemática no desenvolvimento de programas capazes de resolver vários tipos de problemas, isto é, sistemas aptos a pensarem racionalmente (*thinking rationally*). E, por sua vez, há estudos que buscam criar sistemas que sejam eficientes em agir racionalmente, isto é, apresentando a melhor resposta esperada ao operar autonomamente, com a percepção do ambiente e adaptação a mudanças para atingir as metas estabelecidas (*acting rationally*)[42].

Dentre diversas proposições para definir a IA, há cinco que se destacam, as quais seriam pela sua estrutura, comportamento, capacidade, função e princípios. Salienta-se, ainda, que cada uma dessas cinco formas corresponde a um nível diferente de descrição e são listadas

[40] RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022. p. 19.
[41] RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022. p. 19-20.
[42] RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022. p. 20-22.

em ordem crescente em generalidade, como também em ordem decrescente de especificidade[43]. Assim, pela estrutura, em uma abordagem mais centrada no ser humano, o cérebro humano é tomado como inspiração para o desenvolvimento de sistemas semelhantes às suas redes neurais. Embora atualmente seja entendido como impossível se construir artificialmente um cérebro idêntico ao humano, define-se a IA pela proposta de se chegar o mais próximo possível dessa similaridade[44].

Para o comportamento, uma estrutura interna semelhante ao cérebro humano não possui tanta relevância, pois define-se a IA em uma comparação do comportamento do sistema ao comportamento apresentado pela mente humana. Tratando os sistemas de IA e o cérebro como se ambos fossem *black boxes*, para definir a IA importaria verificar se um dito sistema, como no *Turing Test*, é capaz de se comportar como um humano. Um exemplo disso são as tecnologias dos *chatbots*, pelas quais se analisa basicamente o quanto o sistema é capaz de se comunicar como um humano[45].

Por sua vez, pode-se definir a IA através de sua capacidade de resolver problemas difíceis e assim avaliá-la pela utilidade de seus resultados. Por este enquadramento, um sistema é considerado inteligente se é apto a solucionar questões que antes apenas humanos conseguiam. Se apenas o resultado ao final é considerado, é irrelevante verificar se sua estrutura interna e seu comportamento se assemelham aos humanos[46]. Já pela definição pela função, a IA é identificada pelas diferentes funções cognitivas que executa através das entradas de dados e seus resultados manifestados em ações, como pesquisar, tomar decisões e comunicar-se. Na definição pelo princípio, finalmente, entende-se que um sistema de IA segue princípios semelhantes aos que a mente humana apresenta em sua percepções e ações. Aqui, a função é o princípio que rege o sistema de acordo com o seu histórico de atividades, ou seja, como o sistema se comporta e reage em diferentes situações e problemas[47].

---

[43] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 364-368.

[44] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 364.

[45] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 364 – 365.

[46] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023. p. 365.

[47] WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023.

Verifica-se, pois, se quanto ao melhor termo utilizado para se referir à área ainda não há consenso, sobre a definição do que de fato é a inteligência artificial também não há, tendo em vista não haver até o presente momento um claro e universal significado que seja capaz de compreender todas as suas diferentes manifestações. Um dos motivos para essa falta de definição é que a IA não corresponde a um tipo determinado de tecnologia, mas a uma área universal[48], isto é, um conjunto de técnicas e subdisciplinas que envolvem diversas áreas[49], sendo, portanto, um conceito guarda-chuva. Além disso, a depender da área científica em que se baseia, a definição atribuída ao termo IA pode apresentar variações e, consequentemente, produzir efeitos sobre a sua governança[50].

2.2 As definições legais relativas à IA

Para a compreensão e expressão do conceito da IA, recomenda-se a realização de uma abordagem multidisciplinar, considerando que a maneira como se delimita pode gerar impactos diretos em sua regulação, visto que a própria definição já pode se constituir em uma forma de controle. Por isso, de um lado deve ser feita uma análise da temática e de seus reflexos na sociedade, com certa inclinação às ciências sociais e, por outro, valorar alguns fatores para a sua regulação, como o nível de autonomia da IA, a sua capacidade de adaptação e autoaprendizagem, bem como o seu grau de aprendizagem generalizada[51].

No tocante às definições legais da IA no espectro normativo, como forma de compreender e representar a transdisciplinaridade e a complexidade do assunto, vários países e entidades interessadas buscam começar o debate regulatório convocando uma pluralidade de especialistas de diversas áreas do conhecimento. São, portanto, reunidos em grupos, geralmente com competência consultiva, e distribuídos por eixos temáticos heterogêneos, uma vez que

---

[48] RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022. p. 19.

[49] GASSER, Urs; ALMEIDA, Virgilio A.F. **A Layered Model for AI Governance**. IEEE Internet Computing, vol. 21, 2017, 58–62. Disponível em: <https://dash.harvard.edu/handle/1/34390353> Acesso em ago. 2022. p. 2.

[50] LARSSON, Stefan. **On the Governance of Artificial Intelligence through Ethics Guidelines**. Asian Journal of Law and Society, v. 7, n. 3, p. 437–451, 2020. Disponível em: <https://www.cambridge.org/core/journals/asian-journal-of-law-and-society/article/on-the-governance-of-artificial-intelligence-through-ethics-guidelines/992BD33CA7CBBE83E2FBBF6B0179896C> Acesso em ago. 2022. p. 439.

[51] LARSSON, Stefan. **On the Governance of Artificial Intelligence through Ethics Guidelines**. Asian Journal of Law and Society, v. 7, n. 3, p. 437–451, 2020. Disponível em: <https://www.cambridge.org/core/journals/asian-journal-of-law-and-society/article/on-the-governance-of-artificial-intelligence-through-ethics-guidelines/992BD33CA7CBBE83E2FBBF6B0179896C> Acesso em ago. 2022. p. 441.

diversos assuntos e áreas são impactadas pela aplicação da IA em vários seguimentos da atividade econômica e setores da sociedade.

Apresentando diferentes perspectivas sobre os mais variados sistemas de IA com seus respectivos temas e problemas relacionados, esses profissionais tentam juntos construir não somente as definições, como também os princípios e as diretrizes que possam orientar o seu desenvolvimento, implementação e utilização. Além disso, aconselham o Poder Público em suas decisões para o estabelecimento de metas a serem atingidas em diferentes prazos na elaboração de estratégias para o enfrentamento do tema.

Como exemplo, a Organização para a Cooperação e Desenvolvimento Econômico – OCDE apresentou no ano de 2019, através de seu *Committee on Digital Economy Policy – CDEP*, um documento caracterizado como recomendação direcionado aos seus países-membros e países aderentes. No texto, são apresentados princípios para a promoção do uso da IA de forma confiável e em respeito aos direitos humanos e aos valores democráticos, à luz da centralidade do ser humano na abordagem e nos objetivos a serem perseguidos no desenvolvimento da área.

Nessa recomendação, a OCDE apresenta uma definição sobre o que em sua análise viria a ser um sistema de IA, constituindo-se, portanto, em um sistema em uma máquina capaz de, com diferentes níveis de autonomia, atender a metas previamente definidas por humanos, além de fazer previsões, recomendações ou mesmo tomar decisões que podem refletir em ambientes virtuais ou reais[52]. Dentre os princípios propostos, são elencados o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar, valores centrados no ser humano e na imparcialidade, transparência e explicabilidade, robustez, segurança e proteção e prestação de contas[53].

Destaca-se, porque oportuno, que embora os documentos produzidos por organizações internacionais como a OCDE não possuam caráter vinculante, podem ainda assim contribuir para a construção de um sistema de *soft law*[54] com vistas a garantir uma estrutura adequada

---

[52] Conforme o entendimento elaborado pela OCDE, *in verbis*: *"An AI system is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy."* OECD. **Recommendation of the Council on Artificial Intelligence**. Paris: OECD, 21 maio 2019. Disponível em: <https://www.oecd.org/digital/artificial-intelligence/> Acesso em nov. 2022.

[53] OECD. **Recommendation of the Council on Artificial Intelligence**. Paris: OECD, 21 maio 2019. Disponível em: <https://www.oecd.org/digital/artificial-intelligence/> Acesso em nov. 2022.

[54] Termo referente a documentos oriundos do Direito Internacional Público os quais não possuem força normativa nem caráter vinculante, isto é, cujas regras contêm menor valor constringente do que as normas jurídicas.

para os projetos regulatórios em desenvolvimento sobre a IA. Considerando que é um tema que atravessa diversas disciplinas e que seus sistemas ultrapassam fronteiras, a atuação dessas organizações pode colaborar para a apuração de questões técnicas e para a elaboração de relatórios e princípios para seu uso ético e responsável, podendo seus documentos servirem posteriormente como base para produções legislativas em diferentes países[55].

Por sua vez, a União Europeia, buscando manter uma posição pioneira em relação às temáticas do ramo do direito digital, tal como ocorreu com sua regulação sobre proteção de dados pessoais e seu *General Data Protection Regulation – GDPR*, através de sua Comissão Europeia, designou a criação do *High-Level Expert Group on Artificial Intelligence – AI HLEG*[56]. Com competência consultiva e uma composição inclusiva, o grupo é formado por mais de cinquenta peritos amplamente reconhecidos em diferentes campos de atuação, bem como recebe contribuições de diversas entidades interessadas, empresas privadas, instituições acadêmicas e de investigação e até mesmo cidadãos comuns, europeus e estrangeiros.

Assim, o *AI HLEG* colaborou para a elaboração de documentos importantes para o estabelecimento da estratégia em IA do bloco, em vista de se criar um ambiente que estimule o correto funcionamento do mercado interno na área, o principal objetivo da União Europeia em si, nos termos do artigo 114º de seu Tratado de Funcionamento[57]. Mencionam-se as contribuições dadas para a elaboração do *White Paper on Artificial Intelligence*, documento estratégico no qual foram estabelecidas as metas a serem atingidas nas políticas públicas em IA, baseadas na promoção da confiabilidade e no desenvolvimento da área[58], bem como do *Artificial Intelligence Act – AI Act*, projeto de regulação da IA para os países-membros, apresentado no ano de 2021. Tais documentos são o resultado de um exaustivo debate travado pela comunidade europeia ao longo dos últimos anos para a construção de uma proposta que traduza o seu amadurecimento em relação à necessidade e à adequação das suas políticas

---

[55] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 121-122.

[56] EUROPEAN COMISSION. **High-Level Expert Group on Artificial Intelligence**. Brussels, 2022. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> Acesso em mar. 2023.

[57] OFFICIAL JOURNAL OF THE EUROPEAN UNION. **Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2016/C 202/01)**. Lisbon, 2007. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT> Acesso em mai. 2023.

[58] EUROPEAN COMISSION. **White Paper on Artificial Intelligence – A European approach to excellence and trust**. Brussels, 2020. Disponível em: <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf> Acesso em mai. 2023.

públicas para a IA, bem como forneça regras harmonizadas para a sua aplicação no contexto do bloco europeu[59].

Na proposta do *AI Act*, a Comissão Europeia destacou no bojo do considerando número 6 que a definição da expressão "sistemas de IA" utilizada no texto deveria ser, por um lado, inequívoca, em vista de se preservar a segurança jurídica e, por outro, flexível a futuras adaptações de acordo com a evolução tecnológica da IA. Além disso, essa conceituação teria de tomar como base aspectos funcionais dos sistemas, sobretudo a sua capacidade, bem como deveria ser acompanhada por um documento complementar com técnicas e abordagens específicas[60].

À luz do referido documento regulatório, um sistema de IA é compreendido como um programa informático desenvolvido com uma variedade de técnicas e abordagens, sendo capaz de atingir objetivos delineados por seres humanos e apresentar diferentes resultados e conteúdos, como prognósticos, recomendações ou decisões que podem influenciar os mais diversos meios nos quais pode ser inserido.[61] Sendo assim, a União Europeia tenta endereçar não apenas aos seus países-membros, mas a toda a comunidade internacional, uma estrutura regulatória com uma abordagem baseada nos diferentes níveis de risco que os sistemas de IA oferecem, além de estimular a promoção de uma IA de confiança que seja compatível com os valores e interesses do bloco[62].

---

[59] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 141-142.

[60] Segundo o considerando n. 6, *in verbis*: *"The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension. AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to–date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list."* EUROPEAN COMISSION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts**. Brussels, 2021. Disponível em: <https://artificialintelligenceact.eu/the-act/> Acesso em mar. 2023.

[61] No artigo 3°, 1, *ipsis verbis*: *"'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."* EUROPEAN COMISSION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts**. Brussels, 2021. Disponível em: <https://artificialintelligenceact.eu/the-act/> Acesso em mar. 2023.

[62] Ver a seção "1.3 Coerência com as outras políticas da União". EUROPEAN COMISSION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts**. Brussels, 2021. Disponível em: <https://artificialintelligenceact.eu/the-act/> Acesso em mar. 2023.

No entanto, no Brasil essa busca por uma diversidade de profissionais de diferentes áreas científicas não tem sido verificada em todas as iniciativas sobre a IA para o país. Isso porque antes mesmo da apresentação da Estratégia Brasileira de Inteligência Artificial – EBIA por parte do Poder Executivo[63], foi proposto o Projeto de Lei n. 21/2020 na Câmara dos Deputados[64], demonstrando uma certa desarmonia entre os Poderes para o tratamento do assunto. Além disso, tendo sido aprovado no ano de 2021 poucos meses após sua propositura na mencionada casa legislativa sob regime de urgência, claramente não foi oportunizado um amplo debate com diferentes setores da sociedade civil, partes interessadas e até mesmo entre os próprios parlamentares para a devida construção do texto legal.

Embora se propusesse a apresentar diretrizes, fundamentos e princípios para o desenvolvimento e aplicação da IA no país, o referido projeto de lei, intitulado como "Marco Legal da Inteligência Artificial", consiste muito mais em um mero documento principiológico do que uma verdadeira estrutura regulatória como tentava ser. Em pouco mais de dez artigos, o texto se parece mais como uma espécie de plano estratégico a ser seguido pelo Poder Público para a IA e falha em não elencar, por exemplo, a previsão de obrigações e consequentes sanções, bem como mecanismos de supervisão como poderia se esperar de uma norma regulatória[65]. Pelo contrário, constitui-se em um documento vago e carente de força normativa, deixando sempre em aberto para futuras leis o tratamento de diversos assuntos essenciais.

No artigo 2º de seu texto original, o Projeto de Lei n. 21/2020 considera os sistemas de IA como representações tecnológicas das áreas da informática e da ciência da computação, sendo contidos em processos computacionais que operam com base em processamento de dados para atingir metas estabelecidas por humanos, com capacidade para a aprendizagem, percepção, interação e interpretação do ambiente externo. Foram destacadas em seus incisos em rol exemplificativo, ainda, algumas técnicas de IA geralmente utilizadas, como sistemas de aprendizagem de máquina, bem como aqueles baseados em conhecimento ou em lógica, abordagens estatísticas, métodos de pesquisa, dentre outras[66].

---

[63] BRASIL. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Brasília: MCTIC, 2021. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf> Acesso em fev. 2023.

[64] O Projeto de Lei n. 21/2020 é de autoria do deputado federal Eduardo Bismarck.

[65] BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. **AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience**. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 48, n. October 2021, p. 105767, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922001108?via%3Dihub> Acesso em jan. 2023. p. 9.

[66] Artigo 2º, do Projeto de Lei n. 21/2020: Para os fins desta Lei, considera-se sistema de inteligência artificial o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos,

Na elaboração da Estratégia Brasileira de Inteligência Artificial – EBIA também não foi demonstrada uma variedade de fontes colaboradoras que levasse em consideração a complexidade e transdisciplinaridade do tema para a estipulação de metas, juntamente com o devido plano de ações para alcançá-las. O documento contou tão-somente com a participação de profissionais do próprio Governo Federal Brasileiro e do setor privado, além de uma plataforma *online* pela qual as partes interessadas puderam contribuir com comentários sobre vários assuntos em áreas específicas, sem, contudo, terem a possibilidade de integrar as reuniões para construção do plano estratégico, nem ter sido esclarecido que tais contribuições foram devidamente consideradas para a elaboração do documento[67].

Essa pluralidade na discussão da temática apenas foi verificada na atual fase de tramitação do Projeto de Lei n. 21/2020 no Senado Federal Brasileiro. Nesta casa legislativa, a proposta passou a tramitar em conjunto com outras que também objetivam regular a IA, quais sejam, o Projeto de Lei n. 5051/2019 e com o Projeto de Lei n. 872/2021[68]. A fim de elaborarem um texto substitutivo ao aprovado na Câmara, foi designada a criação de uma comissão composta por juristas, juntamente com a participação de diversos profissionais de diferentes áreas relacionadas à IA, como também representantes de entidades do setor privado, de organizações do terceiro setor e de institutos acadêmicos de investigação.

Assim, o texto substitutivo foi apresentado pautado em uma abordagem baseada nos riscos oferecidos pelos sistemas de IA, sendo um modelo regulatório baseado na proteção dos direitos fundamentais, uma vez que o seu propósito é a centralidade no elemento humano, bem como com uma proposta colaborativa, a qual apoia o envolvimento de todas as partes

---

pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões, e que utiliza, sem a elas se limitar, técnicas como: I – sistemas de aprendizagem de máquina (machine learning), incluída aprendizagem supervisionada, não supervisionada e por reforço; II – sistemas baseados em conhecimento ou em lógica; III – abordagens estatísticas, inferência bayesiana, métodos de pesquisa e de otimização. Parágrafo único. Esta Lei não se aplica aos processos de automação exclusivamente orientados por parâmetros predefinidos de programação que não incluam a capacidade do sistema de aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, a partir das ações e das informações recebidas. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 21-A de 2020. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil; e dá outras providências**. Brasília, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9063365&ts=1679601923682&disposition=inline&_gl=1*ejnfbr*_ga*NTQ1OTIzNzcyLjE2NTE3Njg0NDk.*_ga_CW3ZH25XMK*MTY4NTk4NjEzNy4yLjAuMTY4NTk4NjEzNy4wLjAuMA..> Acesso em mar. 2023.

[67] BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. **AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience**. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 48, n. October 2021, p. 105767, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922001108?via%3Dihub> Acesso em jan. 2023. p. 11.

[68] O Projeto de Lei n. 5051/2019 é de autoria do Senador Styvenson Valentim e o Projeto de Lei n. 872/2021 do Senador Veneziano Vital do Rêgo.

interessadas em sua concepção[69]. Em linhas gerais, o documento apresenta como proposta o entendimento legal de que um sistema de IA consiste em um sistema elaborado com diferentes níveis de autonomia para atingir determinados objetivos por meio da análise de dados, inseridos por humanos ou máquinas, sendo que seus resultados, os quais podem ser recomendações, previsões ou decisões, podem ter impactos em ambientes virtuais e reais[70].

Observa-se, assim, que diferentes ordenamentos jurídicos, respeitadas as suas peculiaridades, bem como organizações internacionais, como no mencionado caso da OCDE, têm apresentado uma espécie de consenso com relação ao que se entende acerca dos sistemas de IA, uma vez que não parece haver muita variação sobre a concepção desenvolvida em cada um dos documentos regulatórios mencionados.

Desta forma, verifica-se que os processos regulatórios, onde quer que aconteçam, tendem a esforçar-se para designar grupos de trabalho que compreendam uma diversidade de profissionais de várias origens científicas que tenham ligação com a IA. Além disso, estimulam o amplo debate através da realização de consultas e audiências públicas com a participação de diversos *stakeholders*. Essa pluralidade para a colaboração na discussão é passo fundamental no processo que objetiva criar normas aplicáveis à IA, políticas públicas efetivas, mecanismos de governança e princípios éticos para o devido desenvolvimento, implementação e utilização de suas ferramentas[71].

Uma estrutura normativa que se propõe a regular a IA deve compreender os mais variados impactos que os seus diferentes sistemas podem ocasionar, bem como fornecer um arcabouço legal que proporcione uma proteção aos direitos fundamentais que não se consegue alcançar com as normas já existentes nos ordenamentos jurídicos. Para isso, deve-se levar em

---

[69] SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em mar. 2023. p. 10, 13 e 15.

[70] Nos termos do artigo 4º, inciso I: "sistema de inteligência artificial: sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real." SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em mar. 2023.

[71] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 116.

consideração que a qualidade dessa estrutura regulatória é diretamente afetada pela variedade e qualidade da governança oferecida por essas partes interessadas. Com o envolvimento de diversos setores da sociedade, a regulação da IA pode também contribuir para o enfrentamento de desigualdades causadas e/ou ampliadas pela tecnologia, além de promover a conscientização de toda a sociedade acerca do uso responsável dos sistemas de IA[72].

Por isso, reforça-se a ideia de que a IA é uma ciência plural, construída sobre as bases de várias outras áreas e, a depender da perspectiva pela qual é analisada, pode ser entendida de diversas formas, sem que nenhuma possa ser vista como incorreta. Ademais, é imprescindível compreender que a IA é um campo científico em constante transformação e, por isso, recomenda-se que a própria delimitação de seu conceito não seja feita sem considerar o seu processo de desenvolvimento, bem como seus objetivos e limitações, os quais podem variar conforme o progresso da área e o contexto social, econômico e político em questão.

[72] BELLI, Luca; ZINGALES, Nicolo. **Data protection and artificial intelligence inequalities and regulations in Latin America**. Computer Law & Security Review, v. 47, p. 105761, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922001042> Acesso em jan. 2023. p. 2.

3 OS DARK PATTERNS

Pode ainda não ser possível afirmar se a IA será ou mesmo se já está sendo o melhor ou o pior acontecimento à humanidade[73]. Fato é que a vida atual vem sendo profundamente influenciada e transformada através das inovações tecnológicas nas quais seus sistemas vêm desempenhando importantes papeis, nas mais diversas funções e em diferentes finalidades para as quais são elaborados. Os dados são o núcleo da IA[74], sem os quais muitos tipos de sistemas sequer poderiam ser desenvolvidos, devido a uma profunda relação de dependência de uma enorme variedade, volume e velocidade[75] de coleta e compartilhamento, além do valor, isto é, a qualidade de toda espécie de informação, bem como sua veracidade[76], tendo em vista a extensa circulação de informações falsas e desinformação por todo o ciberespaço.

A informação passou a ocupar uma posição de protagonismo para a economia neste novo modelo de organização social[77], chamado de sociedade da informação[78]. Assim, os dados e, sobretudo aqueles referentes aos usuários, adquiriram valor e passaram a ser objeto de interesse para as mais diversas plataformas, como jogos *online*, *marketplaces* e *streaming* de conteúdos de músicas e filmes, mas especialmente para as redes sociais. Os dados pessoais dos usuários são considerados para muitos o principal produto do modelo de negócio das redes

---

[73] HAWKING, Stephen. **Comments: The Ethics of Artificial Intelligence**. In: BATTRO, Antonio M.; DEHAENE, Stanislas. Power and Limits of Artificial Intelligence. Vatican City: Libreria Editrice Vaticana, 2017. Disponível em: <https://www.pas.va/content/dam/casinapioiv/pas/pdf-volumi/scripta-varia/sv132pas.pdf> Acesso em mai. 2023. p. 50.

[74] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 27.

[75] BARBOSA, Mafalda Miranda. **Inteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos**. 1. ed. Coimbra: Gestlegal, 2021. p. 131.

[76] Sobre os dados que compõem o *Big Data*, T.K., Annavarapu e Bablani mencionam os 5 V's, os quais seriam o volume, velocidade, variedade, veracidade e valor. T.K., Balaji; ANNAVARAPU, Chandra S. R.; BABLANI, Annushree. **Machine learning algorithms for social media analysis: A survey**. Computer Science Review, v. 40, p. 100395, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013721000356> Acesso em ago. 2023. p. 7.

[77] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de janeiro: Forense, 2019. p. 33.

[78] FLORIDI, Luciano. **Information: A Very Short Introduction**. New York: Oxford University Press, 2010.

sociais[79], sendo nos dias de hoje apontados como "o novo petróleo"[80], isto é, uma *commodity*[81] com reconhecido valor econômico no mercado[82]. O interesse sobre eles alia-se a uma necessidade de moderar o conteúdo produzido nessas plataformas, visto que há uma utilidade na manutenção de um ambiente atraente e interessante para que as pessoas sintam-se livres e motivadas a passarem mais tempo conectadas e, consequentemente, a compartilhá-los.

Com a inserção de informações através de suas publicações, tais como fotos e vídeos, bem como opiniões sobre os mais variados tipos de assuntos, além de interações com outros usuários e contas, essas plataformas podem então atrair publicidade e, com isso, gerar receitas e assim movimentar o mercado como um todo[83]. Isso porque podem tanto optar por tratar e analisar tais informações para seus próprios fins, como também vende-los para finalidades diversas[84]. Além das próprias plataformas, há também outras empresas essencialmente especializadas na coleta, mineração, análise e comercialização desses dados[85]. Por isto, tanto através da recolha para a formação de suas próprias bases de dados, bem como pela compra, ou mesmo pela obtenção de informações de domínio público[86], à proporção que as plataformas captam mais dados de seus usuários, mais conseguem ganhar dinheiro[87].

---

[79] IDISIS, Gil'ad. **How to Make Lemonade from Lemons: Achieving Better Free Speech Protection Without Altering the Existing Legal Protection for Censorship in Cyberspace**. Campbell Law Review, v. 36, 2014. Disponível em: <https://scholarship.law.campbell.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1576&context=clr> Acesso em mai. 2023. p. 152.

[80] Hoffman-Rien contesta a utilização metafórica dos dados como "o novo petróleo bruto da sociedade" e elenca cerca de seis teses para sustentar as diferenças entre os dois referidos produtos. Em linhas gerais, embora admita que tal associação busca destacar a sua importância para a economia e a sociedade atual, não são finitos tal como o petróleo, sendo porém expandidos diariamente em todo o mundo. Além disso, não estão escondidos nem requerem complexidade para sua exploração e processamento, dentre outros motivos. HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital: desafios para o direito**. – 2. ed. – Rio de Janeiro: Forense, 2022. p. 22-25.

[81] Para Luciano Floridi, não apenas o dado pessoal, mas a informação como um todo é a *commodity* mais valiosa, para o que ele chama de "sociedade da informação". FLORIDI, Luciano. **Information: A Very Short Introduction**. New York: Oxford University Press, 2010.

[82] BARBOSA, Mafalda Miranda. **Inteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos**. 1. ed. Coimbra: Gestlegal, 2021. p. 134.

[83] DE GREGORIO, Giovanni. **Democratising online content moderation: A constitutional framework**. Computer Law and Security Review, v. 36, p. 105374, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919303851> Acesso em mai. 2023. p. 2.

[84] BÜCHI, Moritz *et al*. **The chilling effects of algorithmic profiling: Mapping the issues**. Computer Law and Security Review, v. 36, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919303784> Acesso em ago. 2023. p. 5.

[85] BARBOSA, Mafalda Miranda. **Inteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos**. 1. ed. Coimbra: Gestlegal, 2021. p. 134.

[86] CORREIA, Pedro; GARCIA, Bruno C. **Inteligência Artificial e Políticas Públicas**. In: PEDRO, Ricardo; CALIENDO, Paulo. Inteligência Artificial no Contexto do Direito Público: Portugal e Brasil. Coimbra: Almedina, 2023. p. 37.

[87] LEE, Kai-fu. QIUFAN, Chen. **Inteligência Artificial 2041: Dez Visões para o Nosso Futuro**. Trad. Maria do Carmo Figueira. Lisboa: Relógio D'Água, 2023. p. 50.

Sem que possamos refletir e decidir, o atual modelo de sociedade que ora se desenvolve, amplamente digital e hiper conectado, está sendo comandado e controlado pelas plataformas que, embora privadas, podem ser consideradas como "novos atores estatais"[88]. Em uma reformulação do sistema econômico capitalista, do qual desponta um "capitalismo de vigilância" sem precedentes, os dados pessoais e comportamentais são coletados de diferentes formas para serem utilizados como matéria-prima, a fim de que essas plataformas sejam capazes de não somente antecipar as vontades e necessidades de seus usuários[89], como também influenciá-las.

Isso porque essas plataformas descobriram que em vez de perceber quais seriam essas tais vontades e necessidades, tendo então que atendê-las, seria mais vantajoso e valioso estabelecer um poder de influência sobre o comportamento de seus usuários, intervindo de acordo com seus interesses de negócios e, por consequência, causando um impacto em toda a sociedade. Em uma relação de assimetria do conhecimento e do poder[90] que essas plataformas têm e exercem sobre seus usuários, suas estruturas digitais são então pensadas para apresentarem em sua arquitetura mecanismos de IA que, além de coletar os dados, possam também induzir seus usuários a tomarem determinadas decisões que originalmente eles não escolheriam. Nessa nova dinâmica imposta, em vez de a IA operar de forma dedutiva, respondendo às interações e atendendo aos comandos, atuando de modo indutivo é ela mesma quem comanda toda a atividade na plataforma[91].

Segundo os princípios tradicionais de boas práticas em *human-computer interaction*[92], o *design* da interface das plataformas, seja em *sites* ou em aplicativos, bem como em qualquer tipo de dispositivo, deveria ser elaborado de modo geral com o objetivo de estimular o engajamento de seus usuários, pelo que se deveria buscar a implementação de uma estrutura eficiente, atraente e acessível. Para isso, deveriam ser aplicados recursos de fácil utilização e informações claras para que a realização de tarefas, em resposta aos comandos dados pelos usuários, ocorresse de forma assertiva e em um curto espaço de tempo. Além disso, a coleta e

---

[88] KLONICK, Kate. **The New Governors: The People, Rules, and Processes Governing Online Speech**. Harvard Law Review, 2018. Vol. 131. Disponível em: <https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf> Acesso em mai. 2023.

[89] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0. p. 14.

[90] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0. p. 15.

[91] BARBOSA, Mafalda Miranda. **Inteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos**. 1. ed. Coimbra: Gestlegal, 2021. p. 132.

[92] *Human-computer interaction (HCI)*, ou interação humano-computador é uma área científica de estudo multidisciplinar que se dedica ao *design* da tecnologia de computadores e outras ferramentas, com foco na interação entre humanos, isto é, os usuários e os computadores.

análise dos dados deveria servir à finalidade de eliminação de erros e melhorias do próprio sistema, de modo a tornar a experiência a melhor possível ao usuário[93]. Em vez de o *design* servir para organizar as informações e opções, passou atualmente a cumprir a função de persuadir e influenciar os usuários a fazerem determinadas ações previamente pensadas pelas empresas[94].

No arranjo imposto pelo capitalismo de vigilância, entende-se que há duas estruturas presentes nas interfaces das plataformas de redes sociais, sendo a primeira aquela à qual os usuários têm acesso e podem simplesmente compartilhar conteúdos e se comunicar com outros usuários. Basicamente, é a concepção comum que as pessoas têm sobre as redes sociais e seu funcionamento. É o que se enxerga delas. Localizada camuflada atrás da primeira, contudo, há uma segunda estrutura a qual se alimenta de todos os dados coletados nas atividades dos usuários na anterior. Assim, sabendo mais sobre os usuários do que talvez eles saibam sobre si mesmos, as plataformas utilizam essas informações para modelar o interesse do público ao seu próprio interesse[95], de forma manifestamente imoral e ilegal[96].

Desta forma, nesta parte do trabalho será abordada a temática dos *dark patterns*, os quais correspondem a elementos de IA inseridos arbitrariamente na interface de usuário de sites, aplicativos e plataformas. Ademais, serão elencados seus diferentes tipos em uma taxonomia, com enfoque especial às espécies majoritariamente encontradas no ambiente virtual das redes sociais.

3.1 A compreensão conceitual e o desenvolvimento histórico dos *dark patterns*

A manipulação de um indivíduo implica na subversão de sua autonomia, isto é, uma influência ou intervenção realizada de maneira indevida e ilegítima para interferir no resultado

---

[93] MERRIT, Kamarin; ZHAO, Shichao. **An Innovative Reflection Based on Critically Applying UX Design Principles**. Journal of Open Innovation: Technology, Market, and Complexity. 2021, 7, 129. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2199853122008988> Acesso em jun. 2023; CONTI, Gregory; SOBIESK, Edward. **Malicious Interface Design: Exploiting the User**. Raleigh: Proceedings of the 19th International Conference on World Wide Web – WWW'10, 2010, p. 271-280. Disponível em: <https://dl.acm.org/doi/10.1145/1772690.1772719> Acesso em jun. 2023. p. 271.

[94] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 14.

[95] Zuboff chama essas estruturas de *"the problem of the two texts"*. ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0. p. 180-181.

[96] MAIER, Maximilian; HARR, Rikard. **Dark design patterns: An end-user perspective**. Human Technology, v. 16, n. 2, p. 170–199, 2020. Disponível em: <https://ht.csr-pub.eu/index.php/ht/article/view/6> Acesso em jun. 2023. p. 171.

de um determinado processo[97]. Assim, as técnicas de manipulação presentes de forma obscura e subliminar nos sistemas de IA que compõem a interface de usuário[98] das plataformas podem ser capazes de arbitrariamente distorcer suas consciências e alterar seus comportamentos. Neste sentido, tais técnicas subliminares são entendidas como ferramentas para, por meio de diferentes estímulos, exercer um poder de influência sobre a consciência das pessoas e seus comportamentos, de modo que o indivíduo não consiga perceber que a referida ação está sendo executada sobre si[99].

Essas práticas enganosas e desleais são conhecidas pelo termo *dark patterns*, um conceito criado por Harry Brignull em meados do ano de 2010 para se referir às interfaces de usuário especialmente concebidas com o propósito de, basicamente, levar os usuários a fazerem determinadas ações[100]. Mais recentemente, outras nomenclaturas também passaram a serem utilizadas e aceitas para mencionar tais práticas, em uma tentativa de evitar associações negativas e estimular o emprego de termos com uma conotação mais inclusiva[101]. Podem ser citados alguns exemplos como *deceptive patterns*, *manipulative patterns*[102], *digital market manipulation*, *sludges*, *evil nudges* ou ainda *dark nudges*[103], além de *asshole design*, *harmfull online choice architecture - OCA*[104] e *persuasive technologies*[105].

Atribuir um significado a essas expressões pode não ser tão fácil, visto que por tratarem de um conceito guarda-chuva, abarcam uma ampla gama de diferentes ferramentas, as quais podem ter finalidades diversas. Isso porque defende-se que, mais importante do que

---

[97] PORTO EDITORA. **"Manipulação" no Dicionário infopédia da Língua Portuguesa** [em linha]. Porto: Porto Editora. Disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/manipulação> Acesso em jun. 2023; DICIONÁRIO DA LÍNGUA PORTUGUESA. **"Manipulação" no Dicionário da Língua Portuguesa**. Academia das Ciências de Lisboa. Disponível em https://dicionario.acad-ciencias.pt/pesquisa/?word=manipulação> Acesso em jun. 2023.

[98] Além do termo "interface de usuário" há o extensivo uso das expressões *user experience design* ou *UX design*, como também *user interface design* ou *UI design*.

[99] BERMÚDEZ, Juan Pablo *et al*. **What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence**. 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS). West Lafayette, United States of America, 2023. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/document/10155039> Acesso em set. 2023.

[100] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 7.

[101] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 17.

[102] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 7.

[103] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 9.

[104] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 17.

[105] FOGG, Brian Jeffrey. **Persuasive technology**. Ubiquity, v. 2002, n. December, p. 2, 2002. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/764008.763957> Acesso em jun. 2023.

desenvolver um conceito que contemple uma definição precisa acerca do tema, é entender que os *dark patterns*, por qualquer nomenclatura que se utilize e de diferentes formas pelas quais sejam empregados, constituem em última instância práticas comerciais desleais que afrontam não somente os direitos dos consumidores[106], mas da sociedade como um todo. Além de não haver acordo sobre o significado do termo em si, pelo que diferentes especialistas e legislações apresentam definições diferentes, também não parece haver consenso sobre se um determinado artifício pode ser propriamente compreendido ou não como um *dark pattern*[107].

Desta forma, vê-se que algumas propostas legislativas que objetivam estabelecer um marco regulatório para a IA e que abordam a temática dos *dark patterns* têm escolhido adotar uma ou outra terminologia. Assim, como exemplo menciona-se que a *Federal Trade Commission – FTC* nos Estados Unidos da América optou por usar em seu *FTC Act* o termo *unfair or deceptive acts or practices* para se referir aos meios de concorrência considerados desleais e, portanto, ilegais que podem afetar o comércio e causar danos previsíveis no país ou que envolvam conduta material ocorrida nos EUA[108]. Por outro lado, em um recente relatório apresentado como resultado de um *workshop* realizado pela referida agência, com o objetivo de orientar a atuação das partes interessadas no assunto em vista da proteção do consumidor, no qual se discutiu o tema buscando entender se e como as interfaces digitais podem ter algum efeito sobre seus usuários, atingindo sua autonomia e comprometendo suas decisões, empregou-se o termo *digital dark patterns*[109].

Já no *Digital Services Act – DSA*, legislação da União Europeia para a regulação de serviços digitais no contexto do bloco, a qual estabelece um conjunto de regras uniformes e proporcionais para o estímulo de um ambiente seguro *online* para seu mercado interno, aliada à proteção dos direitos fundamentais das pessoas, utilizou-se o nome *dark patterns*. Em linhas

---

[106] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report.** Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 28.

[107] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 8.

[108] Segundo o trecho mencionado, *in verbis*: *"(4)(A) For purposes of subsection (a), the term "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that — (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States."* FEDERAL TRADE COMMISSION. **Federal Trade Commission Act incorporating U.S. SAFE WEB Act Amendments of 2006**. Disponível em: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim> Acesso em jun. 2023.

[109] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. United States of America, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-FINAL.pdf> Acesso em jun. 2023.

gerais, no texto o termo é entendido como sendo referente a práticas aptas a provocar a distorção ou prejuízo intencional sobre a capacidade de seus destinatários a tomar decisões informadas e autônomas, sendo portanto empregadas com o objetivo de persuadi-los a fazerem escolhas indesejadas, as quais podem gerar consequências negativas[110].

Com a crescente aplicação dos *dark patterns* espalhados nos mais diversos *sites*, plataformas e aplicativos, a OCDE demonstrou preocupação para com os danos substanciais aos quais os consumidores estariam expostos[111]. Para a organização, os *dark patterns* constituem práticas comerciais que atuam por meio de uma variedade de elementos presentes nas estruturas digitais, especialmente nas interfaces de usuários. Com a exploração de vieses cognitivos e comportamentais, são elaboradas com o objetivo de influenciar as pessoas a tomarem decisões que elas originalmente não fariam, seja por falta de opções, interesse ou mesmo pela ausência de maiores informações[112].

Seus artifícios podem ser identificados em ícones chamativos, relógios com contagem regressiva, ícones e imagens com conotação apelativa, cores diferentes que provocam o destacamento ou até a camuflagem de informações e opções, bem como o posicionamento estratégico dessas informações aliado ao excesso delas ou mesmo sua escassez, além da exploração de sua dubiedade, dentre outros meios. Assim, através de diferentes recursos, buscam atingir a subversão da autonomia dos usuários, comprometendo de modo subliminar suas escolhas[113].

---

[110] Nos termos do considerando n. 67 do *DSA*: *"Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. […]"* EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

[111] A OCDE, através de seu *Committee on Consumer Policy (CCP)*, organizou no ano de 2022 uma reunião para discutir o tema dos *dark patterns*, em vista de se identificar as evidências de sua prática na internet, com seus consequentes danos, bem como para orientar os legisladores na formulação e aplicação de medidas legais para coibi-los. OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 2.

[112] A definição da OCDE para *dark patterns*: *"Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce, or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances."* OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 5.

[113] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-

Mais que as práticas tradicionais existentes no mundo comercial *offline*, sua aplicação no contexto digital torna-se ainda mais preocupante, visto que, ao explorar de forma subconsciente as vulnerabilidades dos usuários, podem oferecer mais riscos[114]. Isso porque diferente do comércio tradicional, nesse novo meio, mais conectado e tecnológico, há fatores como a facilidade de implementação e adaptação de diferentes sistemas de IA com técnicas e objetivos variados, além de uma frequência muito maior e uma escala mais ampla para testar quais recursos podem gerar mais impacto aos usuários[115]. Assim, as tecnologias trouxeram novas e diferentes dimensões, possibilidades e oportunidades de manipulação e persuasão dos consumidores[116].

Faz-se conveniente mencionar, entretanto, que nem sempre os sistemas de IA aplicados nas ferramentas de *design* que resultam em *dark patterns* foram confeccionados com esta exata finalidade, isto é, a pretensão de persuadir e controlar a autonomia dos usuários. Isso porque também pode haver a previsão de desvios de finalidade ou mesmo a ocorrência de erros em *design*, tais como um texto mal redigido que não esclarece as informações ou a disposição de modo confuso das opções disponíveis, os quais, mesmo sem a intenção direcionada, podem converter-se em *dark patterns* e, com isso, ainda gerar lucratividade[117]. Além disso, em alguns casos os *designers* até podem buscar atuar de forma ética no desenvolvimento de seus trabalhos, bem como não ter uma intenção maliciosa, mas enfrentam pressões comerciais para implementar o *design* manipulativo e enganoso[118].

No entanto, torna-se difícil identificar e até mesmo justificar se um determinado sistema de IA com um arranjo em *design* considerado um *dark pattern* foi concebido

---

en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A > Acesso em jun. 2023. p. 5.

[114] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A > Acesso em jun. 2023. p. 5.

[115] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. UNITED STATES OF AMERICA, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800 Dark Patterns Report 9.14.2022 - FINAL.pdf> Acesso em jun. 2023. p. 2; OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A > Acesso em jun. 2023. p. 5.

[116] AHUJA, Sanju; KUMAR, Jyoti. **Conceptualizations of user autonomy within the normative evaluation of dark patterns**. Ethics and Information Technology, v. 24, n. 4, p. 1–18, 2022. Disponível em: <https://doi.org/10.1007/s10676-022-09672-9> Acesso em jun. 2023. p. 3.

[117] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 15.

[118] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A > Acesso em jun. 2023. p. 5, 13.

acidentalmente ou se de fato foi inserido de maneira proposital na arquitetura digital. Em vista disso, na proposta legislativa da União Europeia para a regulação da IA, foi destacado que, se a deturpação do comportamento das pessoas for ocasionada por fatores externos ao sistema de IA implantado, estando por isso fora do controle de seu provedor ou do usuário que com ele interage, essa intenção de distorção pode não ser presumida. Contudo, a pretensão de causar danos não é condição determinante, bastando que esses danos sejam decorrentes das práticas manipuladoras e abusivas dos sistemas de IA[119].

Apesar de que o termo *dark patterns* é de utilização relativamente recente, corresponde a práticas já conhecidas há muito tempo no mercado, sobretudo no campo digital, e que mais atualmente passaram a serem percebidas desta forma[120], isto é, como maliciosas. Entende-se que são o resultado de um processo de três tendências, quais sejam, uma derivada do comércio varejista, outra do campo das investigações em políticas públicas, e uma terceira do ramo do *design*. Desta forma, na primeira compreenderiam as práticas enganosas e manipuladoras as quais oscilam entre o que pode vir a considerado ilegal ao que já foi socialmente normalizado e passou a ser tolerado, embora manifestamente imoral.

Como exemplos dessas estratégias há os falsos anúncios de fechamento de lojas com supostos esvaziamentos de estoques e táticas de *bait and switch*, nas quais evidencia-se no anúncio a qualidade ou o baixo preço de um produto ofertado, mas que ao final não está mais disponível, sendo então substituído por outro de inferior categoria e/ou valor elevado. Além disso, há também o chamado preço psicológico, o qual emprega valores relativamente menores do que um preço com números redondos, causando ao consumidor a falsa sensação de que o bem ou serviço está custando mais barato[121].

---

[119] Segundo o que dispõe o projeto em seu artigo 5, n. 16, nestes termos: *"[...] The intention to distort the behavior may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user, such as factors that may not be reasonably foreseen and mitigated by the provider or the deployer of the AI system. In any case, it is not necessary for the provider or the deployer to have the intention to cause the significant harm, as long as such harm results from the manipulative or exploitative AI-enabled practices. […]"* EUROPEAN PARLIAMENT. **Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM (2021) 0206 – C9 0146/2021 – 2021/0106 (COD))**. 2023. Disponível em: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf> Acesso em jun. 2023.

[120] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 7-9.

[121] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 68-69.

Embora não tenham sido realizadas especialmente focadas em investigar as práticas comerciais de *marketing*, as pesquisas em políticas públicas buscaram compreender de forma geral os comportamentos das pessoas e suas decisões julgadas socialmente como irracionais. Em vista disso, verificou-se a existência de desvios cognitivos capazes de justificar tais comportamentos e escolhas tidos como incongruentes, pelo que seria possível inclusive prevê-los. Assim, esses estudos esclareceram como o comércio, por meio do emprego das técnicas de *nudging*[122], tornou-se capaz, por exemplo, de persuadir os consumidores a pagar a mais por serviços e bens do que efetivamente eles valeriam[123].

Na terceira tendência, finalmente, mais relacionada com os *dark patterns* e com o universo *online*, há o *growth hacking*, isto é, uma estratégia de desenvolvimento de negócios pela qual utilizam-se as ferramentas de *design* para impulsionar um crescimento mais rápido do que normalmente aconteceria em uma expansão gradual[124]. Sendo assim, passou-se a tirar vantagem do resultado das investigações sobre as mudanças de comportamento das pessoas para, através da corrupção desses resultados, intensificar a adoção das técnicas de *nudging* e aplicar a otimização do sistema orientada pelos dados recolhidos[125]. As empresas então entenderam que, ao aproveitarem-se dos vieses cognitivos e comportamentais dos consumidores, seriam capazes de estabelecer uma manipulação do mercado em que atuam e,

---

[122] Em linhas gerais, o *nudging* é entendido como a aplicação de recursos de *design* na interface de usuário que possam orientar a tomada de decisão no ambiente digital, como o estímulo a adoção de determinados comportamentos ou a inclusão de elementos acessíveis a pessoas com diferentes níveis de habilidades. Afirma-se também que esse abordagem funciona justamente porque as pessoas nem sempre se comportam de forma racional, tendo em vista suas limitações cognitivas. Além disso, pode ocasionar diferentes efeitos, a depender das características de cada tomador de decisão. GUNAWAN, Johanna *et al*. **A Comparative Study of Dark Patterns across Web and Mobile Modalities**. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. CSCW2, 2021. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3479521> Acesso em jun. 2023. p. 2; WEINMANN, Markus; SCHNEIDER, Christoph; BROCKE, Jan vom. **Digital Nudging**. Business and Information Systems Engineering, v. 58, n. 6, p. 433–436, 2016. Disponível em: <https://link.springer.com/content/pdf/10.1007/s12599-016-0453-1.pdf> Acesso em jun. 2023. p. 433; JOHNSON, Eric J. *et al*. **Beyond nudges: Tools of a choice architecture**. Marketing Letters, v. 23, n. 2, p. 487–504, 2012. Disponível em: <https://link.springer.com/article/10.1007/s11002-012-9186-1> Acesso em jun. 2023. p. 497.

[123] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 71-72.

[124] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 75.

[125] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 76.

assim, expandir suas possibilidades de obtenção de lucro, com mais sofisticação e efetividade sobre seu público-alvo, além de em uma maior proporção[126].

Por meio de testes[127], verificou-se que mudanças substanciais nas arquiteturas dos *sites*, plataformas e aplicativos poderiam interferir na autonomia dos usuários, levando-os a alterarem seus comportamentos e decisões e assim fazerem exatamente o que a plataforma espera que eles façam[128]. Isso porque deve-se levar em consideração a dificuldade em estabelecer uma neutralidade na forma de se apresentar as opções disponíveis ao usuário, sem que esse arranjo possa interferir em seu livre-arbítrio e, consequentemente, em sua escolha[129], visto que geralmente o que é escolhido depende de como as alternativas são oferecidas[130].

Em vista disso, ao explorar os resultados das pesquisas comportamentais, os *dark patterns* foram sendo desenvolvidos como uma consequência dos problemas éticos do *design* das interfaces de usuário emergidos em meio a uma crise entre os valores da sociedade e das empresas[131], considerando a falta de consenso existente sobre uma definição clara acerca do que seria um *design* ético[132]. Por isso, o *design* passou então a ser utilizado como um ardiloso

---

[126] MATHUR, Arunesh *et al*. **What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods**. Conference on Human Factors in Computing Systems - Proceedings, 2021. Disponível em: <https://doi.org/10.48550/arXiv.2101.04843> Acesso em jun. 2023. p. 9.

[127] Os testes aplicados geralmente são no formato A/B, no qual são apresentadas aos usuários diversas versões, ainda que com diferenças sutis, para verificar qual interface performa melhor de acordo com as métricas estabelecidas para cada modelo de negócio, mesmo que os resultados possam vir a causar danos aos usuários. Esse tipo de teste não aponta qual modelo é melhor ou pior para o usuário, mas fornece os dados estatísticos para posterior análise sobre qual pode gerar um maior impacto segundo os interesses do negócio. NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 75-77; OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 13; BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 23.

[128] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 77.

[129] WEINMANN, Markus; SCHNEIDER, Christoph; BROCKE, Jan vom. **Digital Nudging**. Business and Information Systems Engineering, v. 58, n. 6, p. 433–436, 2016. Disponível em: <https://link.springer.com/content/pdf/10.1007/s12599-016-0453-1.pdf> Acesso em jun. 2023. p. 434.

[130] JOHNSON, Eric J. *et al*. **Beyond nudges: Tools of a choice architecture**. Marketing Letters, v. 23, n. 2, p. 487–504, 2012. Disponível em: <https://link.springer.com/article/10.1007/s11002-012-9186-1> Acesso em jun. 2023. p. 488.

[131] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 81.

[132] DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023.

artifício de fácil controle e ajuste para ampliar a lucratividade[133] e assim atender aos escusos objetivos do capitalismo de vigilância[134].

Os *dark patterns* podem ser entendidos como um desvirtuamento dos princípios tradicionais de *design*[135], aplicáveis em avaliações heurísticas de usabilidade das interfaces de usuário[136]. Isso porque tais enunciados estabelecem regras gerais para que o *design* da área de interação entre o sistema e o usuário seja intuitivo e de fácil utilização[137]. Tais preceitos são (i) a visibilidade do status do sistema, (ii) a combinação entre o sistema e o mundo real, (iii) o controle e a liberdade do usuário, (iii) a consistência e os padrões e (iv) a prevenção de erros. Além destes, há também (vi) o reconhecimento em vez da recordação, (vii) a flexibilidade e a eficiência de uso, (viii) o *design* estético e minimalista, (ix) o auxílio ao usuário para reconhecer, diagnosticar e corrigir erros e, finalmente, (x) a ajuda e documentação.

Desta forma, em vez de seguir o princípio, tal como recomendado em seu enunciado, subverte-se o seu sentido para fazer exatamente o contrário[138] e tirar o máximo proveito do resultado disso. Assim, ao invés de utilizar uma linguagem clara e objetiva, por exemplo, com palavras comuns e até mesmo expressões do cotidiano do usuário, usam-se palavras de duplo sentido para dificultar a compreensão dos termos e condições e das opções disponíveis. No lugar de um *design* estético e minimalista, exibe-se uma interface extravagante, cheia de detalhes, cores chamativas e janelas que só são fechadas quando se executa o que o sistema

---

[133] BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023. p. 10.

[134] NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em: jun. 2023. p. 79.

[135] BRIGNULL, Harry. **Dark Patterns: inside the interfaces designed to trick you**. The Verge, 2013. Disponível em: <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> Acesso em jun. 2023.

[136] Segundo Nielsen e Molich, há quatro maneiras de se analisar a usabilidade do *design* da interface de um determinado site ou plataforma, isto é, o quanto essa área de interação entre o sistema e o usuário é de fácil utilização pelos seus destinatários. Assim, a avaliação formal é realizada através da aplicação de alguma técnica específica, a automática é feita utilizando um procedimento computadorizado, enquanto na análise empírica são aplicados testes ao usuário e na heurística simplesmente observa-se o sistema e sua interface e apontam-se considerações a respeito. NIELSEN, Jakob; MOLICH, Rolf. **Heuristic evaluation of user interfaces**. Conference on Human Factors in Computing Systems - Proceedings, n. April, p. 249–256, 1990. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/97243.97281> Acesso em jun. 2023.

[137] Nielsen e Molich desenvolveram nove enunciados, posteriormente atualizados para dez, nos quais recomendavam princípios a serem seguidos pelos desenvolvedores de sistemas de IA e *designers*. NIELSEN, Jakob; MOLICH, Rolf. **Heuristic evaluation of user interfaces**. Conference on Human Factors in Computing Systems - Proceedings, n. April, p. 249–256, 1990. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/97243.97281> Acesso em jun. 2023; NIELSEN, Jakob. **10 Usability Heuristics for User Interface Design**. Nielsen Norman Group, 2020. Disponível em: <https://www.nngroup.com/articles/ten-usability-heuristics/> Acesso em jun. 2023.

[138] BRIGNULL, Harry. **Dark Patterns: inside the interfaces designed to trick you**. The Verge, 2013. Disponível em: <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> Acesso em jun. 2023.

pede, como fornecer dados pessoais para subscrição. Em vez de apresentar uma arquitetura que permita a utilização pelo usuário de forma livre e com controle sobre suas decisões, confundem-se as opções para que suas ações incorram em erros que, ao final, de um jeito ou de outro sempre venham a beneficiar os resultados do negócio.

Isso porque o maior objetivo dos *dark patterns* é expandir a lucratividade das empresas a todo custo, tanto nas vendas de seus produtos como em receitas de publicidade[139] e, por isso, é fundamental que se aplique a subversão da autonomia das pessoas e exerça controle sobre suas decisões. Assim, são capazes de alterar a consciência das pessoas e, consequentemente, seu comportamento, levando-os a ações que elas originalmente não fariam, como fornecer mais dados, mais dinheiro e mais tempo de atenção do que efetivamente seria da sua vontade ou até mesmo necessidade[140]. Com diferentes abordagens ocultas e técnicas de manipulação e persuasão, os *dark patterns* cumprem sua função sem que os consumidores tenham sequer conhecimento de que estão sendo manipulados e enganados[141].

3.2 Uma taxonomia sobre os *dark patterns* identificados nas redes sociais

Os *dark patterns* costumam ser inseridos nas interfaces de usuário com a aplicação de diversas formas e abordagens, bem como com diferentes propósitos, a depender do modelo de negócio em questão, além da utilização das tecnologias de IA através das técnicas, por exemplo, de *machine learning*[142]. Assim, podem servir para coletar mais dados pessoais do que o essencial para ter acesso a um produto, levar os consumidores a gastar mais dinheiro em produtos desnecessários nos *sites*, plataformas e aplicativos, bem como ocupar mais tempo

---

[139] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 8.

[140] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 5.

[141] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. USA, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-_FINAL.pdf> Acesso em jun. 2023. p. 3.

[142] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023. p. 9.

conectados vendo informações que não são do seu interesse, além de também perder tempo tentando encontrar uma explicação clara para tomar decisões informadas.

Comumente, os *dark patterns* não são adotados isoladamente, sendo porém introduzidos em combinação com diferentes tipos[143], o que pode levar a um incremento do impacto e dos efeitos produzidos e, consequentemente, dos danos gerados às pessoas. Considerando que as empresas utilizam diversas técnicas de coletas de dados não somente sobre seus consumidores, mas acerca de seu público-alvo como um todo, com as informações necessárias em mãos torna-se mais fácil desenvolver sistemas de IA e diversificar as estratégias para atingir "os alvos certos"[144].

Embora os *dark patterns* estejam presentes dispersos por praticamente toda a internet, verifica-se uma maior regularidade em dispositivos móveis, principalmente nas versões de aplicativos de plataformas do que nos seus formatos *mobile websites* ou *desktop websites*[145]. Além disso, seus resultados pode ser intensificados a depender do tipo de equipamento pelo qual o *site* e/ou a plataforma são acessados, visto que através de telas menores, como no caso dos celulares e *tablets*[146], aparentam ter maior efetividade sobre os usuários do que em telas maiores como em computadores[147].

Com a crescente multiplicidade de práticas comerciais maliciosas identificadas como *dark patterns*, verifica-se que muitas investigações até propõem-se a coletar e analisar as suas mais diferentes espécies. No entanto, percebe-se uma inconsistência e ausência de clareza nas conceituações presentes na literatura sobre o tema[148], além de que considera-se improvável de

---

[143] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 6.

[144] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. USA, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-_FINAL.pdf> Acesso em jun. 2023. p. 2.

[145] GUNAWAN, Johanna *et al*. **A Comparative Study of Dark Patterns across Web and Mobile Modalities**. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. CSCW2, 2021. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3479521> Acesso em jun. 2023.

[146] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. USA, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-_FINAL.pdf> Acesso em jun. 2023. p. 3.

[147] Utz *et al* realizaram um estudo sobre o impacto dos avisos de consentimento de *cookies* em *sites* após a entrada em vigor do Regulamento Geral de Proteção de Dados na União Europeia. Verificou-se que a posição do aviso na tela, além das opções e do estímulo oferecidos e do texto apresentado podem significar uma interferência no comportamento e na escolha dos usuários, a qual pode ter resultados diferentes em dispositivos móveis como celulares e tablets do que em computadores. UTZ, C. *et al*. **(Un)informed Consent: Studying GDPR consent notices in the field**. Proceedings of the ACM Conference on Computer and Communications Security, p. 973–990, 2019. Disponível em: <https://arxiv.org/pdf/1909.02638.pdf> Acesso em jun. 2023.

[148] MATHUR, Arunesh *et al*. **What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods**. Conference on Human Factors in Computing Systems - Proceedings, 2021. Disponível em: <https://doi.org/10.48550/arXiv.2101.04843> Acesso em jun. 2023. p. 5.

se catalogar e definir todos os seus possíveis tipos de maneira exaustiva, embora muitos modelos sejam apresentados como diferentes quando na verdade apenas foram identificados com outros termos e novas expressões.

Isso se deve ao fato de que a todo momento, com os avanços tecnológicos, sobretudo no ramo da IA com o desenvolvimento de novos sistemas e algoritmos, bem como com a adaptação e o aprimoramento dos já existentes, podem surgir novas modalidades em novos formatos de interface de usuário. Ademais, em cada levantamento e classificação podem ser apresentados vieses de acordo com os objetivos de cada pesquisa e os critérios adotados para admitir uma ou outra técnica como um *dark pattern*, como por exemplo observando-se os tipos de danos causados, o público-alvo ou com relação ao dispositivo escolhido. Até mesmo a estratégia e o procedimento empregados para identificar tais práticas podem interferir em sua análise e resultado[149].

Considerando que as redes sociais correspondem ao escopo da presente investigação, analisar-se-ão os *dark patterns* apontados pela literatura como predominantes no referido ambiente digital. Desta forma, verificam-se que as doze seguintes práticas costumam ter maior incidência no referido modelo de negócio, quais sejam, (i) o *infinite scroll*, (ii) o *autoplay design*, (iii) *preselection by default*, (iv) *hidden information*, (v) *false hierarchy* e (vi) *disguised ad*. Do mesmo modo, há também grande presença de técnicas de (vii) *roach motel*, (viii) *forced registration*, (ix) *nagging*, (x) *toying with emotion*, (xi) *intermediate currency* e (xii) *activity messages*[150].

Uma prática escassamente relacionada na literatura, mas talvez uma das mais perigosas em *dark patterns*, o artifício chamado de *infinite scroll*, *infinite scrolling* ou *endless scrolling*

---

[149] OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A > Acesso em jun. 2023. p. 11.

[150] No ano de 2022 a Comissão Europeia apresentou um relatório, no âmbito do Programa da União Europeia para Consumidores, no qual foi realizado um estudo comportamental sobre as práticas comerciais desleais presentes no campo digital, sobretudo no que tange aos *dark patterns* e a personalização de conteúdo com intenções manipuladoras. Dentre diferentes formas relatadas de se classificar os *dark patterns*, a pesquisa propôs uma análise com base no tipo de *website* ou aplicativo e verificou as espécies mais frequentes em cerca de quatorze *websites* ou aplicativos utilizados no bloco europeu dos tipos de comunicação, relacionamento, mídia social e rede social. Dentre os examinados estão plataformas como o *Facebook, TikTok, Instagram, Pinterest, Twitter, Bumble, Badoo, Snapchat, WhatsApp Messenger, Facebook Messenger, Viber Messenger* e *Gmail*. Assim, o mencionado levantamento faz referência à realidade do contexto europeu, mas que, considerando a natureza multinacional das redes sociais, as quais são em geral largamente utilizadas em todo o mundo, pode corresponder as suas interfaces de usuário apresentadas em seus serviços em outros países. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022.

consiste em um padrão de *design* inserido na interface de usuário no qual é disponibilizada uma rolagem infinita de conteúdo na página sem a necessidade de cliques[151]. Ao funcionar como uma espécie de *slot machine*, na qual ao rolar para baixo novas publicações são mostradas, seu intuito é manter o usuário conectado por mais tempo ao *site* e/ou plataforma, de modo que seja possível consumir o máximo de conteúdo disponível[152].

Desta forma, tendo a atenção das pessoas, consegue-se fazer com que elas forneçam mais dados pessoais através de suas interações na plataforma, gastem mais dinheiro adquirindo bens e serviços e, mais que isso, passem a se interessar sobre aquilo que o algoritmo de recomendação não somente apresenta, mas induz que seja do seu interesse. Mais que um hábito, é um *dark pattern* que pode levar ao vício, isto é, tornar o usuário dependente e obcecado pela plataforma e em ficar mais tempo conectado a ela, embora também possa ser visto por alguns pesquisadores como apenas irritante[153].

Outro mecanismo muito presente nas redes sociais, mas pouco trabalhado pela literatura sobre *dark patterns* é o *autoplay design* ou apenas *auto-play*, uma configuração de reprodução automática pela qual os arquivos de mídia, especialmente os de vídeo, são exibidos continuamente[154]. Assim, o sistema algorítmico apresenta mais e mais conteúdo, relacionados ou não ao vídeo assistido anteriormente[155], mas associado ao assunto que a plataforma recomenda por considerar que é interessante a cada tipo de usuário. Como geralmente o *autoplay* é uma configuração padrão do sistema, é também percebido como um padrão ruim, visto que dificulta ou até mesmo não possibilita sua modificação[156], fazendo com que o usuário

---

[151] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 67.

[152] HARRIS, Tristan. **The Slot Machine in your Pocket**. Spiegel International, 2016. Disponível em: <https://www.spiegel.de/international/zeitgeist/smartphone-addiction-is-part-of-the-design-a-1104237.html> Acesso em jul. 2023.

[153] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 108.

[154] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al.* **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 67.

[155] MILLER, Katharine. **Can't Unsubscribe? Blame Dark Patterns**. Stanford University. Human-Centered Artificial Intelligence, 2021. Disponível em: <https://hai.stanford.edu/news/cant-unsubscribe-blame-dark-patterns> Acesso em jul. 2023.

[156] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 108.

se mantenha conectado por mais tempo à plataforma e tendo acesso a conteúdos que podem não ser realmente do seu interesse.

Um dos mais frequentes *dark patterns* não somente nas redes sociais, mas em vários tipos de *sites*, plataformas e aplicativos é o *preselection by default*. É considerado como uma interferência na interface do usuário, na qual são favorecidas certas ações em detrimento de outras[157], para confundir o usuário ou mesmo dificultar o encontro de informações importantes[158]. São então oferecidas opções já pré-selecionadas pelo sistema, tornando-as uma configuração padrão, podendo ou não ser possível alterá-las. Essa técnica explora os vieses cognitivos do chamado "efeito padrão", pelo qual as pessoas tendem a aceitar a escolha previamente definida pelo sistema, mesmo que tenham outras disponíveis, por entender que outras pessoas supostamente também teriam aquela mesma preferência[159]. Ao influenciar a livre tomada de decisão do usuário, o resultado disso é que ele pode ser conduzido a aceitar determinadas alternativas e conceder permissões que originalmente podem não corresponder a sua vontade[160].

Geralmente constituem opções desfavoráveis ao consumidor[161], visto que fornece um suposto consentimento à empresa para que realize certas ações, como a coleta de mais dados pessoais do que efetivamente seria necessário para o regular funcionamento do sistema e a execução de atividades pelo usuário, além de proceder ao envio de notificações e comunicações por e-mail, *push* e/ou mensagens de texto, bem como concordar com o armazenamento de arquivos de *cookies* a respeito das operações realizadas na plataforma. No que tange aos *cookies* do sistema ao usuário no *design preselection by default*, em muitos casos há avisos informando sobre a sua recolha sem sequer apresentar alternativas de interação, isto é, para aceitar ou negar. Assim, há certas plataformas nas quais, se o usuário continua a navegar pela página, isso pode ser interpretado como uma concordância, uma anuência. Além disso, pode também ser exibida

---

[157] MAIER, Maximilian; HARR, Rikard. **Dark design patterns: An end-user perspective**. Human Technology, v. 16, n. 2, p. 170–199, 2020. Disponível em: <https://ht.csr-pub.eu/index.php/ht/article/view/6> Acesso em jun. 2023. p. 179.

[158] GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 7.

[159] DECEPTIVE PATTERNS. **Preselection**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/preselection> Acesso em jul. 2023.

[160] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 269, 283.

[161] DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023. p. 3.

apenas uma única opção como “OK” ou “eu concordo”[162], o que também pode ser visto como um aparente consentimento.

Mais uma técnica amplamente aplicada de interferência na interface de usuário, em *hidden information* ou *hidden options* uma informação importante é visualmente ocultada ou exibida de tal forma que seja difícil a sua localização pelo usuário, para estimular a seleção de uma opção desejada pelo sistema[163]. Com o disfarce das informações camufladas através de textos geralmente descoloridos, confundindo-se com as cores de fundo da tela, bem como letras pequenas ou mesmo a inclusão de várias informações irrelevantes misturadas àquelas consideradas importantes para o usuário nos termos e condições de uso da plataforma[164], o objetivo é claramente dificultar a acessibilidade às opções e informações relevantes[165].

Já na técnica de *false hierarchy*, prioriza-se uma opção, destacando-a por exemplo com cores brilhantes, letras maiores ou fontes diferentes para induzir o usuário a selecioná-la[166], ou seja, a decidir pelo que sistema considera que é melhor, em vista dos seus objetivos próprios. Ao conceder uma precedência visual ou interativa a uma alternativa em detrimento de outras, cria-se a aparência de que a opção evidenciada é a única disponível ou que está em uma posição hierarquicamente superior em relação às demais[167], isto é, que é supostamente a melhor escolha, manipulando assim a autonomia do usuário e sua livre tomada de decisão.

Um dos mais populares e disseminados na internet e muito presente nas redes sociais, no padrão obscuro de *disguised advertising* ou simplesmente *disguised ad*, sua estratégia

---

[162] UTZ, C. *et al*. **(Un)informed Consent: Studying GDPR consent notices in the field**. Proceedings of the ACM Conference on Computer and Communications Security, p. 973–990, 2019. Disponível em: <https://arxiv.org/pdf/1909.02638.pdf> Acesso em jun. 2023. p. 3.

[163] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 45, 64.

[164] GRAY, C. M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 7.

[165] NELISSEN, Lei; FUNK, Mathias. **Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments**. International Journal of Design, v. 16, n. 1, p. 75–92, 2022. Disponível em: <http://www.ijdesign.org/index.php/IJDesign/article/view/4117> Acesso em jul. 2023. p. 83.

[166] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 45.

[167] GRAY, C. M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 7.

consiste na manipulação de informações[168] e de estética[169], uma vez que é admitido como uma interferência na interface[170]. Nessa prática, são inseridos anúncios de publicidade de maneira disfarçada entre outros tipos de publicações, como se fossem elementos do próprio *design* da interface de usuário[171], tais como botões, opções e formulários.

A página é apresentada como uma espécie de campo minado, no qual qualquer clique ou toque podem levar a um *download* ou ao carregamento de outra página, transformando a tela inteira em um grande anúncio publicitário[172]. Nas redes sociais, o conteúdo patrocinado disfarçado engana as pessoas visto que costuma aparecer como se fosse uma publicação compartilhada por um usuário mas que, ao clicar, redireciona para a página de um anunciante, dentro ou fora da plataforma[173]. Embora problemático e considerado como uma das práticas abusivas mais prejudiciais aos consumidores por parte da literatura[174], por outra parte é visto como apenas moderadamente ruim, mas que ainda assim pode ocasionar em consequências danosas aos consumidores[175].

Conhecido como *roach motel*, *hard opt-out*, *hard to cancel*, *obstruction* ou *forced work*, é um *dark pattern* considerado de esforço assimétrico[176]. Em um primeiro momento há uma certa facilidade para realizar a assinatura ou registro de uma conta ao serviço oferecido por

---

[168] AHUJA, Sanju; KUMAR, Jyoti. **Conceptualizations of user autonomy within the normative evaluation of dark patterns**. Ethics and Information Technology, v. 24, n. 4, p. 1–18, 2022. Disponível em: <https://doi.org/10.1007/s10676-022-09672-9> Acesso em jun. 2023. p. 9.

[169] GRAY, C. M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 7.

[170] DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023. p. 3.

[171] ÖZDEMIR, Şebnem. **Digital nudges and dark patterns: The angels and the archfiends of digital communication**. Digital Scholarship in the Humanities, v. 35, n. 2, p. 417–428, 2020. Disponível em: <https://academic.oup.com/dsh/article-abstract/35/2/417/5372748?redirectedFrom=fulltext> Acesso em jul. 2023. p. 419.

[172] MICHAELS, Jordyn. **Pathways to the Light: Realistic Tactics to Address Dark Patterns**. Rutgers Computer & Technology Law Journal, vol. 49, Nbr. 1, March 2023. Disponível em: <https://law-journals-books.vlex.com/vid/pathways-to-the-light-921006230> Acesso em jul. 2023. p. 181.

[173] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 50.

[174] TJOSTHEIM, Ingvar *et al*. **Dark Pattern: A Serious Game for Learning About the Dangers of Sharing Data**. Proceedings of the European Conference on Games-based Learning, v. 2022- October, p. 774–783, 2022. Disponível em: <https://nla.brage.unit.no/nla-xmlui/handle/11250/3025227> Acesso em jul. 2023. p. 779.

[175] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 107.

[176] AHUJA, Sanju; KUMAR, Jyoti. **Conceptualizations of user autonomy within the normative evaluation of dark patterns**. Ethics and Information Technology, v. 24, n. 4, p. 1–18, 2022. Disponível em: <https://doi.org/10.1007/s10676-022-09672-9> Acesso em jun. 2023. p. 52.

uma determinada plataforma, mas que posteriormente torna quase impossível para o usuário que saia ou desista de uma situação, tais como cancelar uma subscrição ou excluir um perfil[177].

Como em uma espécie de jogo de manipulação, este padrão costuma enganar o usuário ao confundi-lo com a falsa sensação de controle da situação, tendo em vista a praticidade oferecida para entrar e acessar o produto. Porém, quando demonstrada a vontade de encerrar a relação, a dinâmica é totalmente invertida para que a plataforma dificulte ao máximo a resolução, passando de um processo dentro do seu sistema para diversas etapas, envolvendo ou não a participação ou mesmo dependência de decisão humana para a sua conclusão[178]. Ao impor o cumprimento de várias fases até o encerramento total da situação, o consumidor é levado a perder mais tempo e, em muitos casos, chega até a sua desistência[179], o que pode repercutir em gastos desnecessários de dinheiro, no fornecimento de mais dados pessoais e ao vínculo a um serviço que não corresponde ao seu desejo.

No padrão identificado como *forced registration*, *forced action* ou *forced enrollment*, também compreendido como de esforço assimétrico[180], o usuário é levado a aceitar que para utilizar o serviço oferecido deve preliminarmente passar por um complexo processo de inscrição à plataforma[181]. Ao limitar a autonomia e a tomada de decisão, funciona como uma condição de permuta, na qual é apresentado ao consumidor algo que é do seu interesse, mas que para obtê-lo necessita antes de fazer ou dar algo em troca[182], o que no caso é o acesso aos seus dados pessoais e a vinculação ao serviço.

Já no *dark pattern* denominado como *nagging*, a tarefa realizada pelo usuário na página é continuamente interrompida para que ele proceda à ação desejada pela plataforma, o

---

[177] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 107.

[178] BARONI, Luiz Adolpho *et al*. **Dark Patterns: Towards a Socio-technical Approach**. ACM International Conference Proceeding Series, 2021. Disponível em: <https://dl.acm.org/doi/abs/10.1145/3472301.3484336> Acesso em jul. 2023. p. 3.

[179] DECEPTIVE PATTERNS. **Hard to cancel**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/hard-to-cancel> Acesso em jul. 2023.

[180] AHUJA, Sanju; KUMAR, Jyoti. **Conceptualizations of user autonomy within the normative evaluation of dark patterns**. Ethics and Information Technology, v. 24, n. 4, p. 1–18, 2022. Disponível em: <https://doi.org/10.1007/s10676-022-09672-9> Acesso em jun. 2023. p. 52.

[181] CONTI, Gregory; SOBIESK, Edward. **Malicious Interface Design: Exploiting the User**. Raleigh: Proceedings of the 19th International Conference on World Wide Web – WWW'10, 2010, p. 271-280. Disponível em: <https://dl.acm.org/doi/10.1145/1772690.1772719> Acesso em jun. 2023. p. 272-273; GUNAWAN, Johanna *et al*. **A Comparative Study of Dark Patterns across Web and Mobile Modalities**. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. CSCW2, 2021. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3479521> Acesso em jun. 2023. p. 9.

[182] DECEPTIVE PATTERNS. **Forced action**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/forced-action> Acesso em jul. 2023.

que se repete até que ele ceda[183]. Geralmente consiste em avisos de áudio ou no formato *pop-up*[184], os quais podem, por exemplo, requerer uma permissão para o envio de notificações por *push*, *e-mail* ou mensagem de texto, para rastrear a localização do dispositivo utilizado, para acessar o álbum de mídia de fotos e vídeos do aparelho, para que sejam compartilhados os seus contatos[185], convidar amigos ou mesmo para que seja feita a atualização do serviço gratuito para uma versão paga[186]. Além disso, podem solicitar a anuência sobre os termos e condições de uso da plataforma, como também a reconsideração de escolhas e respostas negativas dadas anteriormente[187].

Embora compreendido como moderadamente ruim[188], é uma estratégia de interação coercitiva entre o usuário e o sistema[189], pois funciona como um mecanismo de exaustão do consumidor, tendo em vista que ao interromper a atividade do usuário, esgota seu tempo e sua atenção, obrigando-o a executar a ação que a plataforma deseja[190]. Isso porque nem sempre as opções são claras como "sim" ou "não", mas costumam ser apresentadas como "permitir", "consentir" e "aceitar" para respostas positivas e como "mais tarde", "não agora", "pedir ao app para não rastrear", "salvar" ou "confirmar minhas escolhas" como as negativas. Assim como o padrão de *forced registration*, é um dos *dark patterns* mais inseridos nas redes sociais e com

---

[183] GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 5; MATHUR, Arunesh *et al*. **What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods**. Conference on Human Factors in Computing Systems - Proceedings, 2021. Disponível em: <https://doi.org/10.48550/arXiv.2101.04843>
Acesso em jun. 2023. p. 4.

[184] DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023. p. 5.

[185] GUNAWAN, Johanna *et al*. **A Comparative Study of Dark Patterns across Web and Mobile Modalities**. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. CSCW2, 2021. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3479521> Acesso em jun. 2023. p. 9.

[186] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 53.

[187] NEWMAN, Stephen J.; DENSON, Allen H.; MA, Jimmy L. **Potential First Amendment Defenses to a Dark Patterns Claim**. Intellectual Property & Technology Law Journal, v. 35, n. 4, 2022. Disponível em: <https://www.stroock.com/uploads/Newman-Denson-Ma-copy1.pdf> Acesso em jul. 2023. p. 10.

[188] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 108.

[189] GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 8.

[190] DECEPTIVE PATTERNS. **Nagging**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/nagging > Acesso em jul. 2023.

maior aceitabilidade pelos consumidores, visto que preferem ceder à pressão realizada pela plataforma a continuar sendo incomodados com a mesma notificação várias vezes[191], mesmo que isso seja contra seus interesses.

Também considerado como moderadamente ruim, quando comparado a outras espécies de *dark patterns*, o padrão *toying with emotion* ou *selectively biased examples*[192] consiste em uma interferência na interface[193], visto que se apresenta como uma estrutura de *design* que se utiliza da manipulação das emoções do usuário[194]. Para brincar com os sentimentos dos consumidores, são empregados diversos tipos de linguagem, associados a um estilo, cor e destaque, bem como outros elementos como figuras que possam provocar algum abalo moral ou afetivo, seja de forma fofa, desprezível ou até mesmo assustadora, a fim de persuadi-los a agir conforme os interesses da plataforma[195]

Embora para uma parte da literatura não seja admitida necessariamente como um *dark pattern*, na técnica de obstrução chamada *intermediate currency*, o usuário é forçado a utilizar uma espécie de moeda virtual para processar as transações dentro da plataforma, o que pode ocasionar em uma ocultação dos custos realizados. Assim como costuma ser feito nesse tipo de tática, pela qual torna-se um processo mais complexo de como deveria ser, obrigando o consumidor a tomar certas ações, dificulta-se a sua capacidade em calcular o real valor gasto no produto[196]. Seu objetivo é justamente confundir o usuário para que ele se desconecte da

---

[191] MAIER, Maximilian; HARR, Rikard. **Dark design patterns: An end-user perspective**. Human Technology, v. 16, n. 2, p. 170–199, 2020. Disponível em: <https://ht.csr-pub.eu/index.php/ht/article/view/6> Acesso em jun. 2023. p. 187.

[192] CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em: <https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023. p. 107.

[193] DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023. p. 3.

[194] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 30.

[195] GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 7.

[196] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 35, 51.

realidade, levando-o a interagir e consumir de forma diferente do que ocorreria com a moeda oficial corrente[197].

Por fim, a prática denominada *activity messages*, *testimonials* ou *fake social proof* consiste no envio de mensagens e notificações para apresentar uma informação, falsa ou mesmo verdadeira, sobre a atividade de outras pessoas na plataforma. Assim, ao descrever a ações e a experiência de outros consumidores, sua intenção é influenciar o comportamento do usuário para que ele se sinta motivado ou até mesmo pressionado para fazer o que os demais estão supostamente fazendo, como se fosse uma espécie de prova social[198].

Portanto, verifica-se que, utilizando diferentes técnicas com distintas abordagens e geralmente em conjunto, as redes sociais buscam manter os seus usuários conectados e atendendo aos seus próprios interesses, sem se importar que para isso terão que aplicar mecanismos escusos de manipulação, coerção, persuasão e até falsidade inseridos na interface de interação entre o sistema e o usuário. De forma sutil ou mesmo persistente e perturbadora, o intuito não é impor descaradamente uma mudança de comportamento nas pessoas, mas levá-las a isso, produzindo um novo comportamento que possa conduzir às suas finalidades comerciais, as quais, quaisquer que sejam, devem gerar lucro[199].

Considerando que as doze diferentes espécies de *dark patterns* ora relatadas possuem características, objetivos e aplicações peculiares, para a sua melhor compreensão organizar-se-ão todas, de forma resumida e objetiva, na tabela a seguir. Destaca-se, porque oportuno, que a intenção em mencionar como exemplo uma ou mais redes sociais em cada um dos tipos de padrões estudados tem a proposta de demonstrar como a sua utilização tornou-se comum e está espalhada de diversas maneiras nas mais variadas plataformas de redes sociais.

---

[197] GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023. p. 6.

[198] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022. p. 289.

[199] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0. p. 194-195.

TIPO	DESCRIÇÃO	OBJETIVO	APLICAÇÃO
Infinite scroll	Rolagem infinita de conteúdo na página	Manter o usuário conectado por mais tempo à plataforma, para coletar seus dados pessoais	*Feed* de notícias do *Facebook*, no qual quando o usuário se aproxima do fim da página, o sistema ativa automaticamente a requisição de novas publicações
Autoplay	Reprodução automática de arquivos de mídia de vídeo e imagem	Manter o usuário conectado por mais tempo à plataforma, para coletar seus dados pessoais	*For You* do *TikTok* ou *Reels* do *Instagram*, nos quais o usuário passa apenas o dedo e os vídeos são reproduzidos automaticamente
Preselection by default	Pré-seleção padrão de opções pelo sistema, com a possibilidade ou não de alteração	Fazer com que o usuário aceite a opção desejada pelo sistema	Aba de "convites de conexão" no *Linkedin*, na qual a opção para permitir convites de todos os usuários da plataforma é pré-selecionada e indicada como recomendada, podendo ser alterada.
Hidden information	Disfarce e ocultação de informações e/ou opções importantes	Fazer com que o usuário aceite a opção desejada pelo sistema	*Termos de Uso/Aceite* das redes sociais, com excesso de informações em linguagem de difícil compreensão. Apenas é possível criar a conta e aceitar nos termos em sua integralidade.
False hierarchy	Destaque intencional de uma opção em detrimento de outras	Fazer com que o usuário aceite a opção desejada pelo sistema	Central de contas da *Meta*, a qual é destacada dentre as demais opções de configurações de perfil de usuário, a fim de levá-lo a fazer escolhas que impactem em todas as contas que possui nos aplicativos da referida empresa.
Disguised advertising	Inserção de anúncios de publicidade disfarçados entre outros tipos de publicações	Levar o usuário a consumir os produtos dos anunciantes	*Stories* do *Instagram*, nos quais as publicações de publicidade direcionada são exibidas continuamente e entre as publicações de outros usuários
Roach motel	Processo assimétrico de fácil inscrição à plataforma, mas de difícil processamento de exclusão da conta	Forçar a desistência do usuário com a consequente continuidade do vínculo ao serviço da plataforma	Processo de exclusão de conta no *Facebook*, no qual a aba "menu"

			apresenta várias opções listadas, mas não é visivelmente fácil de encontrar a opção de exclusão da conta, sendo visível apenas a alternativa de simplesmente sair do aplicativo, o que não significa a sua exclusão.
Forced registration	Inscrição compulsória à plataforma para acessar seus recursos	Vinculação do usuário à plataforma para coletar seus dados pessoais	A grande maioria das redes sociais, como *Facebook*, *Linkedin*, *Instagram* e *TikTok* funciona por meio da aplicação deste *dark pattern*, pois a visualização de páginas e perfis é limitado e condicionada à inscrição.
Nagging	Interrupção contínua da atividade na plataforma para que seja executada uma ação	Fazer com que o usuário aceite a opção desejada pelo sistema	Aviso de notificação dentro do *Instagram* para permitir o compartilhamento dos *Stories* também em seu perfil no *Facebook*, quando as contas de um usuário em ambas as redes são conectadas. Mesmo que o usuário já tenha decidido que não ou que apenas quer fazê-lo uma vez, continua a receber tal requerimento.
Toying with emotion	Emprego de elementos de *design* como linguagem apelativa, cores, figuras e ícones para provocar abalo moral ou sentimental no usuário	Fazer com que o usuário aceite a opção desejada pelo sistema	Processo de encerramento de conta no *Linkedin*, no qual a plataforma informa que lamenta a decisão do usuário e que com isso ele perderá o acesso a contatos, como empresas e pessoas de sua rede.
Intermediate currency	Utilização de uma moeda virtual obrigatória para transações dentro da plataforma	Confundir o usuário para que gaste mais dinheiro na plataforma	*Facebook Stars*, no *Facebook*, pela qual um usuário pode enviar dinheiro a um outro, sendo este criador de conteúdo, através de estrelas e presentes virtuais animados. Não é possível comprar apenas uma estrela, somente

			pacotes e seu custo depende da quantidade comprada.
Activity Messages	Envio de mensagens e notificações com a informação, verdadeira ou falsa, sobre a atividade de contatos e/ou outras pessoas na plataforma	Impulsionar o acesso e a utilização do usuário à plataforma, estimulando a atividade e interação com outros usuários	Notificações do *Linkedin*, pelas quais o usuário é continuamente avisado sobre a atividade e a atualização de outras pessoas e contas que ele siga na plataforma

Tabela 1: Compêndio dos *dark patterns* mais presentes nas redes sociais[200]

Fonte: Autora

[200] Segundo os dados analisados em um comportamental sobre as práticas comerciais desleais presentes no campo digital realizado pela Comissão Europeia. Vide nota de rodapé n. 144. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, Francisco *et al*. **Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022.

4 AS QUESTÕES E CONSEQUÊNCIAS RELATIVAS À APLICAÇÃO DOS *DARK PATTERNS* NAS REDES SOCIAIS

Costuma-se afirmar que se um dado serviço ou produto é gratuito, que então o produto é o próprio usuário[201]. Em um primeiro momento, as plataformas de redes sociais aparentam oferecerem uma vasta gama de produtos e serviços de forma gratuita, popularmente conhecido como modelo *freemium*[202], apesar de que em algumas, para acessar certas funcionalidades podem ser requeridas assinaturas mediante pagamento. O fato de ofertarem suas aplicações de graça, repletas de ferramentas e possibilidades, foi o que popularizou o seu uso e impulsionou o seu crescimento[203]. No entanto, trata-se apenas de uma mera aparência, tendo em vista que o preço por sua utilização pode custar muito mais caro do que se o valor fosse cobrado essencialmente em dinheiro.

Isso porque esse suposto pagamento é feito por meio da coleta de toda sorte de dados relativos aos usuários através de sua inscrição compulsória, já que praticamente não é possível participar de uma rede social sem a total adesão aos seus termos e condições de uso, tampouco transigir acerca de suas cláusulas, bem como obtêm-se dados por intermédio de todas as atividades realizadas na plataforma. Além da recolha dos dados pessoais, o custo da gratuidade de seus serviços advém também das receitas obtidas em publicidade direcionada e pela definição de perfis comportamentais, pela técnica conhecida como *profiling*[204]. Desta forma, em vez de ser constituída uma relação bilateral nos moldes tradicionais envolvendo o consumidor, ora usuário, e a plataforma, estabelece-se uma conexão plurilateral, para que também sejam contempladas as empresas anunciantes de conteúdo publicitário, as quais são justamente quem financia todo esse arranjo de negócio[205].

Assim, esses dados são adquiridos por meio dos acessos à plataforma e tudo o que é possível obter através de cada ação executada, desde suas informações pessoais, sua

---

[201] A expressão popular *"if something is free, you're the product"* não possui autor determinado ou conhecido, pelo que apresenta diversas divergências quanto à sua autoria.
[202] A expressão *"freemium*" refere-se à combinação entre as palavras em inglês *free*, ou seja, gratuito, e *premium*, algo diferenciado, exclusivo. BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de janeiro: Forense, 2019. p. 48.
[203] LANIER, Jaron. **Ten Arguments for Deleting your Social Media Accounts Right Now**. 1. ed. New York: Henry Holt and Company, 2018. p. 68.
[204] BIETTI, Elettra. **A Genealogy of Digital Platform Regulation**. Georgetown Law Technology Review, 1, 2023. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859487> Acesso em ago. 2023. p. 30.
[205] BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de janeiro: Forense, 2019. p. 47.

localização, o tipo de aparelho pelo qual se usa, bem como o horário e as interações com outros usuários. Além disso, também coletam-se as informações relativas às reações, emoções e expressões faciais (se autorizado o acesso à câmera) referentes às decisões tomadas a cada atividade realizada, opção ou publicação exibida, dentre outras maneiras, como fazendo uso da coleta da voz em segundo plano, isto é, quando a plataforma não está plenamente em uso mas continua em execução (se autorizado o acesso ao microfone do dispositivo).

Com base nesses dados, essas empresas podem então não somente elaborar os mecanismos de IA certos e direcionados para seus objetivos de negócio, sendo com isso capazes de moldar o interesse do seu público, como também testá-los, treiná-los e adaptá-los de acordo com as suas necessidades e conveniências. Assim, através da defraudação do *design* de suas interfaces de usuário pela aplicação dos *dark patterns* em seus mais variados formatos, realizam tais experimentos disponibilizando diferentes funcionalidades e opções ardilosamente manipuladas e, supostamente, com o rótulo da personalização, para atingir determinados grupos de pessoas.

Todo indivíduo conectado pode ser um alvo em potencial, visto que para as empresas há múltiplas razões e maneiras para enquadrar cada um em um determinado segmento ou em um público específico, ou seja, para tornar alguém de um simples alvo a plenamente consumidor, de acordo com as intenções do mercado. Mencionam-se como "alvos", a título de exemplificação, os menores, os idosos, os jovens, as pessoas residentes em uma certa localidade ou de uma dada classe social, bem como os frequentadores de um certo local ou estabelecimento, o público que navega na plataforma em específicos horários ou por determinadas modalidades de acesso (tais como em seus modelos de aplicativos para computador, *smartphone* ou *tablet*, em *mobile websites* ou *desktop websites*).

Como em um laboratório no qual os animais são objeto de estudo e ensaios científicos, pelo que se busca provar certas hipóteses e lograr determinados objetivos por meio de experimentações e da análise de suas reações, as quais possam interferir em sua vontade e resposta em cada teste e, com isso, ocasionar a modificação de seus comportamentos, os usuários são vistos e tratados pelas redes sociais como meros animais de laboratório[206]. Desta forma, sob o domínio do capitalismo de vigilância, não é a rede social que está sendo personalizada para cada usuário segundo suas preferências e escolhas, é o usuário que está sendo manipulado e moldado de acordo com as expectativas e interesses de negócio de cada

[206] LANIER, Jaron. **Ten Arguments for Deleting your Social Media Accounts Right Now**. 1. ed. New York: Henry Holt and Company, 2018. p. 9-10.

plataforma e suas empresas responsáveis[207]. A combinação entre a distorção da consciência das pessoas e, consequentemente a alteração de seus comportamentos e decisões com a utilização maciça de meios tecnológicos, tal como a inserção dos *dark* patterns e a utilização de mecanismos de *machine learning*, é parte essencial desse recente sistema que se impõe como novo modelo econômico e social.

Um dos principais objetivos das redes sociais é estimular a atividade de seus usuários na plataforma, no que chamam popularmente de engajamento. Sua finalidade é justamente gerar mais dados pessoais, como por exemplo para o aprimoramento de seus sistemas de recomendações, tendo em vista que há uma relação diretamente proporcional entre a quantidade de acessos e as ações executadas, com as informações captadas e a receita possível de ser obtida através disso[208]. Para isso, suas arquiteturas digitais são meticulosamente formuladas para atrair mais atenção e assim fomentar a participação das pessoas, utilizando-se de sistemas de IA e todos os artifícios tecnológicos possíveis para manter o usuário conectado por mais tempo.

Ressalta-se que a utilização dos sistemas de IA pode trazer benefícios significativos para as empresas, pois podem desempenhar um importante papel para o funcionamento das mais variadas plataformas de redes sociais. Considerando a grande quantidade de dados gerados a todo o instante graças ao volumoso número de usuários ativos[209] e suas intensas atividades e conexões, reputa-se ser quase impossível de se gerir todo o conteúdo sem o auxílio dessas ferramentas, apenas contando com a ação humana. Em vista disso, os mecanismos como o *machine learning* são amplamente utilizados como métodos estatísticos para, em um primeiro momento coletar os dados necessários e, posteriormente, realizar suas análises e assim identificar os padrões e as relações entre os dados. Dentre suas diversas aplicações, podem ser elaborados levantamentos para a detecção de anomalias nos sistemas, verificação de imagens e vídeos e recomendações de publicações, tanto de usuários como de publicidade, além de

---

[207] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0. p. 278; EG, Ragnhild; DEMIRKOL TØNNESEN, Özlem Demirko; TENNFJORD, Merete Kolberg. **A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors**. Computers in Human Behavior Reports, v. 9, n. November 2022, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2451958822000872?via%3Dihub> Acesso em ago. 2023. p. 1.

[208] SAURA, José Ramón; PALACIOS-MARQUÉS, Daniel; ITURRICHA-FERNÁNDEZ, Agustín. **Ethical design in social media: Assessing the main performance measurements of user online behavior modification**. Journal of Business Research, v. 129, n. March, p. 271–281, 2021. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0148296321001545> Acesso em: jun. 2023. p. 272.

[209] Estima-se que atualmente há cerca de 4,62 bilhões de usuários ativos nas maiores plataformas de redes sociais, o que corresponde a 58% por cento da população mundial, sendo as mais utilizadas o *WhatsApp*, o *Facebook* e o *Instagram*. WE ARE SOCIAL. **The Global State of Digital in October 2022**, 2022. Disponível em: <https://wearesocial.com/us/blog/2022/10/the-global-state-of-digital-in-october-2022/> Acesso em ago. 2023.

análises de sentimentos, emoções e opiniões e avaliações comportamentais[210] para então, com base nesses relatórios, ser possível fazer as previsões necessárias para cada finalidade, a fim de melhorar os serviços oferecidos.

Assim, por um lado, há metodologias e técnicas de *machine learning* aplicadas para transformar os dados coletados nessas plataformas em informação útil para o aprimoramento da eficiência de seus bens e atividades e o auxílio na tomada de decisão. Dentre muitas possibilidades de aplicação, podem ser mencionadas como exemplos as técnicas de *business intelligence*, pela qual as empresas buscam compreender seus consumidores e o impacto de seus produtos e serviços por meio da análise de sua avaliação nas redes sociais. Há também as análises comportamentais, através de metodologias de *natural language processing, opinion mining* e *text mining*, pelas quais são elaborados relatórios com base na observação das interações entre as pessoas nas redes sociais, sendo possível, por exemplo, resolver problemas e até mesmo prevenir que atividades criminosas sejam realizadas na plataforma[211].

Por outro lado, entretanto, há o extenso uso das ferramentas e métodos estatísticos de *machine learning* para fins maliciosos, tornando seus resultados de positivos a potencialmente danosos e, dentre diversas possibilidades de aplicações negativas, encontram-se os *dark patterns*, tendo por consequência muitos efeitos prejudiciais aos direitos fundamentais das pessoas. Isso porque através dessas técnicas, inseridas propositalmente de forma subliminar nas arquiteturas das plataformas, torna-se viável para elas assumirem um controle sobre o conteúdo a que cada usuário é exposto, ocasionando assim em uma interferência em suas preferências e em toda sua atividade e, dessa forma, na proteção e no exercício de seus direitos.

Em vista disso, dentre outros possíveis desdobramentos e consequências refletidas por cada aplicação mencionada no capítulo anterior, neste segmento a pesquisa concentrar-se-á sobre a questão da personalização do conteúdo e sua relação com os *dark patterns*. Assim, analisar-se-á como isso é feito por meio da aplicação de tais práticas manipuladoras no *design* das redes sociais, em especial aquelas desenvolvidas para manter o usuário conectado pelo máximo de tempo possível à plataforma, a fim de serem coletadas suas informações pessoais para a elaboração de perfis comportamentais. A despeito de não ser o escopo desta investigação, tratar-se-á da temática do *profiling* na medida em que tais métodos automatizados relacionam-

---

[210] T.K., Balaji; ANNAVARAPU, Chandra S. R.; BABLANI, Annushree. **Machine learning algorithms for social media analysis: A survey**. Computer Science Review, v. 40, p. 100395, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013721000356> Acesso em ago. 2023. p. 8.

[211] T.K., Balaji; ANNAVARAPU, Chandra S. R.; BABLANI, Annushree. **Machine learning algorithms for social media analysis: A survey**. Computer Science Review, v. 40, p. 100395, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013721000356> Acesso em ago. 2023. p. 9-11 e 25.

se com os *dark patterns* estudados, além de que serão analisadas também as interferências ocasionadas pelo uso maciço de tais ferramentas no exercício e proteção de alguns direitos e liberdades fundamentais.

4.1 A linha tênue entre a personalização de conteúdos e a manipulação do usuário: o problema envolvendo o *profiling* e os *dark patterns* de *infinite scroll* e o *autoplay design*

De uma forma geral, a personalização pode ser entendida como positiva para o consumidor, visto que possibilita o acesso a um serviço ou produto, o qual pode ser customizado de modo parcial ou total às suas preferências, interesses e necessidades, carregando por isso um caráter de singularidade, isto é, uma exclusividade. No entanto, quando se fala da personalização do conteúdo exibido pelas redes sociais, o entendimento pode ser diverso, uma vez que como já mencionado, é o usuário que passa a ser "personalizado", por meio da ação dos algoritmos, segundo os objetivos de negócio das empresas. Assim, em vez de melhorar o serviço oferecido, o sistema de recomendações e a personalização do conteúdo podem ocasionar efeitos prejudiciais às pessoas e aos seus direitos fundamentais, visto que através de seus filtros, exercem um poder de controle sobre o acesso a informações e publicações, manipulando os resultados exibidos, isto é, ao dar prioridade a postagens consideradas interessantes para o utilizador em detrimento de outras[212].

Note-se que nem toda personalização de conteúdo em plataformas pode ser compreendida como negativa e ruim ao usuário, pois o sistema de recomendações pode tanto melhorar a qualidade do serviço ofertado[213], quanto fazer parte do próprio serviço em si, isto é, quando não há o envolvimento de terceiros anunciantes e patrocinadores. Plataformas de outros nichos de mercado como de *streaming* de filmes, séries e documentários, a exemplo da *Netflix* e da *Disney Plus*, bem como de *streaming* de música e *podcasts* como o *Spotify*, funcionam

---

[212] EG, Ragnhild; DEMIRKOL TØNNESEN, Özlem Demirko; TENNFJORD, Merete Kolberg. **A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors**. Computers in Human Behavior Reports, v. 9, n. November 2022, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2451958822000872?via%3Dihub> Acesso em ago. 2023. p. 1.

[213] PEI, Huining *et al*. **A personalized recommendation method under the cloud platform based on users' long-term preferences and instant interests**. Advanced Engineering Informatics, v. 54, n. May, p. 101763, 2022. Disponível em: < A personalized recommendation method under the cloud platform based on users' long-term preferences and instant interests - ScienceDirect> Acesso em ago. 2023. p. 2.

seguindo as preferências do usuário para oferecer as sugestões mais adaptadas com base nos seus gostos e gêneros favoritos[214].

Em toda atividade e interação com a plataforma, o usuário está fornecendo dados pessoais para alimentar os algoritmos e, com isso, ajuda a ajustar o sistema de recomendações de publicações. Deste modo, com base em aspectos como informações demográficas, hábitos e preferências, histórico de compras e pesquisas e as ações de seus contatos ou mesmo de outras pessoas com características parecidas, assim como também em fatores desconhecidos[215], tendo a vista a *black box* existente dentro desses sistemas[216], além de outros atributos já referenciados, ao aplicar a ideia de que "se você gosta disto, vai gostar daquilo também", tomam decisões que resultam no que é exibido a cada indivíduo.

Para isso, os dados coletados são analisados e então reunidos em perfis comportamentais por meio da implementação das técnicas de *profiling* ou *automated algorithmic profiling*, que correspondem ao processamento automatizado da verificação de associações entre os dados presentes em um certo banco. Em âmbito legal, o *profiling* é entendido pela União Europeia, nos termos do artigo 4, parágrafo 4 do *General Data Protection Regulation - GDPR*, como sendo qualquer método de tratamento automatizado de dados pessoais cuja finalidade seja a avaliação de determinados fatores da pessoa titular para estabelecer previsões relacionadas ao seu comportamento, saúde, preferências e interesses, desempenho profissional, dentre outros aspectos[217].

---

[214] LANIER, Jaron. **Ten Arguments for Deleting your Social Media Accounts Right Now**. 1. ed. New York: Henry Holt and Company, 2018. p. 26.

[215] EG, Ragnhild; DEMIRKOL TØNNESEN, Özlem Demirko; TENNFJORD, Merete Kolberg. **A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors**. Computers in Human Behavior Reports, v. 9, n. November 2022, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2451958822000872?via%3Dihub> Acesso em ago. 2023. p. 1.

[216] Costuma-se mencionar que os sistemas algoritmos possuem uma *black box* interna, porque nem mesmo seus próprios desenvolvedores são capazes de explicar com clareza como operam, sendo, portanto, sistemas fechados que recebem a informação (*input*) e produzem um resultado (*output*) sem justificar suas decisões. YU, Ronald; ALÌ, Gabriele Spina. **What's Inside the Black Box? AI Challenges for Lawyers and Researchers**. Legal Information Management, v. 19, n. 01, p. 2–13, 2019. Disponível em: <https://www.cambridge.org/core/journals/legal-information-management/article/whats-inside-the-black-box-ai-challenges-for-lawyers-and-researchers/8A547878999427F7222C3CEFC3CE5E01> Acesso em ago. 2023.

[217] Segundo o artigo 4, parágrafo 4 do GDPR, *in verbis*: *"'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."* EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

Assim, esses perfis podem ser utilizados para a identificação e/ou representação de um sujeito, podendo com isso individualizar, representar ou mesmo relacionar alguém como membro de um grupo ou uma categoria de pessoas[218]. Em outras palavras, através das aplicações de *machine learning* para *data mining*, o *profiling* produz uma nova noção, ou seja, um novo entendimento sobre um conhecimento já existente, a partir da análise das correlações dos dados referenciados[219]. Os perfis produzidos são, por sua vez, aplicados para desenvolver um conhecimento preditivo sobre os indivíduos, isto é, uma espécie de relatório de probabilidade, cuja função consiste em auxiliar na tomada de decisão estratégica, pelo que podem ser construídos e diferenciados segundo as correlações e análises realizadas.

O processamento das informações pelo *profiling* acontece essencialmente em duas fases, sendo a primeira o momento de descoberta da informação, na qual é feita a recolha de grandes conjuntos de dados, passando ao tratamento para um determinado formato, para que então esses dados tenham condições de utilização, bem como a sua análise, a fim de se detectar os padrões e as relações existentes, os quais convertem-se na construção dos perfis. Por sua vez, a segunda fase abrange a própria aplicação dos perfis elaborados para previsões e decisões, de acordo com as finalidades estabelecidas[220].

Desta forma, em uma concepção técnica, os perfis elaborados podem ser caracterizados como individuais e de grupo, bem como em diretos e indiretos. Os perfis individuais identificam e representam uma pessoa em específico; já os perfis de grupo, como a própria nomenclatura sugere, correspondem a uma associação de pessoas em determinado, podendo serem ainda classificados como distributivos, isto é, quando os indivíduos de um conjunto apresentam os mesmos atributos, e não-distributivos, quando são verificados que certos aspectos não são visualizados em todos os integrantes. Podem ainda haver os perfis diretos, o que significa que os dados coletados são referentes a um sujeito ou comunidade em especial e que sua aplicação dar-se-á apenas a eles, bem como perfis indiretos, os quais envolvem a recolha e análise de informações de uma reunião ampla de pessoas[221].

---

[218] NEUWIRTH, Rostam J. **Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)**. Computer Law and Security Review, v. 48, p. 105798, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000092> Acesso em ago. 2023. p. 10.

[219] BÜCHI, Moritz *et al*. **The chilling effects of algorithmic profiling: Mapping the issues**. Computer Law and Security Review, v. 36, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919303784> Acesso em ago. 2023. p. 2.

[220] YEUNG, Karen. **Algorithmic Regulation: A Critical Interrogation**. King's College London Dickson Poon School of Law. Legal Studies Research Paper Series. n. 2017-27, p. 1–45, 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505> Acesso em ago. 2023. p. 22.

[221] FERRARIS, Valeria; BOSCO, Francesca; D'ANGELO, Elena. **The Impact of Profiling on Fundamental Rights**. SSRN Electronic Journal, p. 1–45, 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753> Acesso em ago. 2023. p. 4.

Os perfis produzidos pelas técnicas de *profiling* são feitos por decisões automatizadas de sistemas de IA utilizados para classificar, categorizar e avaliar pessoas, as quais na maioria das vezes não possuem o mínimo consentimento necessário ou sequer conhecimento a respeito de seus resultados e possíveis consequências. Por isso, geralmente não há a alternativa de contestar tais resultados, nem mesmo a possibilidade de aferir sua eficácia[222]. Em muitos casos, as pessoas nem mesmo têm noção de que uma determinada decisão, cujos impactos interferem de alguma forma em sua vida, foi tomada com base na análise de um perfil, diretamente construído com seus dados ou indiretamente, através de uma comparação com outros indivíduos.

Verifica-se que o próprio funcionamento da plataforma acontece a partir desses perfis comportamentais elaborados, em uma combinação com a aplicação dos *dark patterns*. Em uma espécie de processo circular, em um primeiro momento há a implantação de tais mecanismos manipuladores na arquitetura digital das redes sociais, como o *infinite scroll* e o *autoplay design*, os quais são responsáveis por reter ao máximo a atenção do utilizador. Por meio de tais técnicas, é então feita a coleta de todas as informações possíveis relativas ao usuário para a confecção dos perfis. Por sua vez, com o *profiling* definido, estabelecem-se as previsões de quais seriam as publicações mais prováveis de atingir as finalidades da plataforma, isto é, tanto manter o usuário conectado por mais tempo, bem como selecionar quais anúncios de publicidade teriam maior impacto e resultariam em compras. Finalmente, com a análise desses resultados, passa a atuar o sistema de recomendações e personalização do conteúdo, fazendo o direcionamento das publicações mais adequadas para satisfazer a tal propósito, isto é, consumir sua atenção, para recolher mais dados pessoais e fazê-lo gastar dinheiro com os bens e serviços anunciados. Assim, com as publicações selecionadas, entram em ação os *dark patterns*, no intuito de manter o usuário conectado por mais tempo, liberando mais dados e visualizando as postagens direcionadas. É como um ciclo de manipulação sem fim, o qual pode ser visualizado de forma sintética a partir da figura a seguir.

[222] PRIVACY INTERNATIONAL; ARTICLE 19. **Privacy and Freedom of Expression in the Age of Artificial Intelligence**. April, 2018. Disponível em: <https://privacyinternational.org/sites/default/files/2018-04/Privacy and Freedom of Expression In the Age of Artificial Intelligence.pdf> Acesso em ago. 2023.

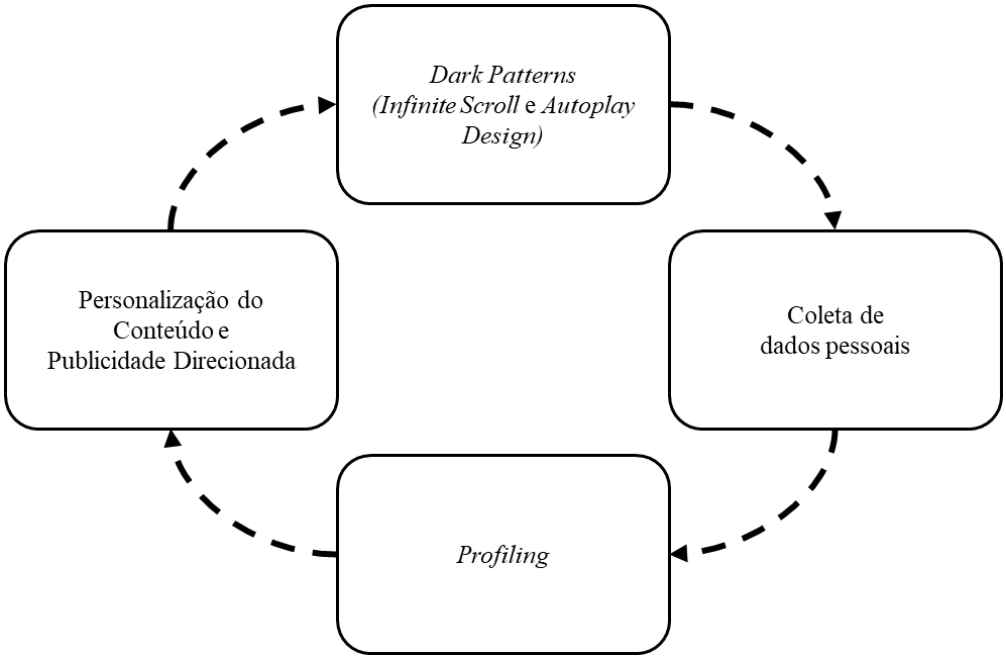

Figura 1: Funcionamento cíclico das redes sociais

Fonte: Autora

Assim, por meio dos dados apurados pelo *profiling*, é possível, por exemplo, direcionar as notícias com as informações sobre uma determinada cidade ou região aos seus cidadãos, encaminhar aos eleitores e/ou simpatizantes de um líder político ou partido os seus discursos, bem como da mesma forma também informá-los sobre os ideais defendidos, as demandas necessárias e as expectativas de seus eleitores sobre suas manifestações públicas e ações. Ademais, possibilita que anúncios de publicidade sejam destinados aos consumidores de um determinado bem ou serviço ou de um certo nicho de mercado, de acordo com suas preferências[223], aumentando sua efetividade[224], assim como exibe com favoritismo as publicações dos contatos e demais contas com as quais o usuário tem mais interações, em detrimento das demais.

Executa-se, então, um processo dividido em três partes, sendo a primeira a fase em que a plataforma descobre quem é o usuário, seus interesses e preferências. Posteriormente, são exibidos os conteúdos que, segundo tais informações, teriam maior probabilidade de serem

[223] VILLANI, Cédric. **Artificial Intelligence – Big Achievements and Huge Questions Viewed from Mathematics**. In: BATTRO, Antonio M.; DEHAENE, Stanislas. Power and Limits of Artificial Intelligence. Vatican City: Libreria Editrice Vaticana, 2017. Disponível em: <https://www.pas.va/content/dam/casinapioiv/pas/pdf-volumi/scripta-varia/sv132pas.pdf> Acesso em ago. 2023. p. 34.

[224] SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. New York University Press, 2004. p. 19.

aceitos e, por fim, o próprio usuário se ajusta ao conteúdo reproduzido. Assim, como resultado, ao passo em que a identidade de uma pessoa e tudo relacionado a ela podem moldar o conteúdo da rede social, por outro lado a rede social também molda o seu usuário[225], mudando-o de acordo com seus interesses. Haveria, desta forma, uma relação recíproca entre os usuários e os algoritmos, uma vez que apresentam resultados com base em prognósticos, ou seja, previsões sobre as pessoas e seus comportamentos, as quais, por sua vez, passam a tentar compreender e dar sentido a tais resultados, adaptando-se a eles, o que demonstra o poder de manipulação, influência e controle que o sistema é capaz de exercer sobre as pessoas a ele conectadas[226].

No entanto, verifica-se que ao manipular a atividade e o comportamento de seus usuários na plataforma, impondo com isso uma precedência visual a determinados tipos de publicações em detrimento de outros, bem como utilizando-se dos anúncios de publicidade direcionada específicos de certos segmentos de mercado, surgem diversos problemas às pessoas. Com o sistema de personalização de conteúdo atuando como a causa e o efeito desse processo[227], cria-se uma espécie de redoma informacional, na qual o usuário é levado continuamente a ter acesso a um restrito tipo de postagem e, mais que isso, a pensar que os conteúdos personalizados de sua rede social são o reflexo de sua identidade e correspondem à realidade como um todo.

Ao controlar o que as pessoas veem ou não, no chamado *"filter bubble"*[228], envolve-se a realidade em um manto de invisibilidade, o que resulta na distorção da percepção acerca da verdade, exercendo uma interferência na relação entre os indivíduos e o exercício de seus direitos fundamentais, seu livre-arbítrio e o ambiente social do qual fazem parte. O usuário é, em vista disso, inserido em um universo de informações totalmente limitado e adaptado para si, isto é, uma zona de conforto informacional[229] e, com isso, levado a crer que todas as opções que lhe estão disponíveis são as únicas existentes, comprometendo com isso suas habilidades de escolha e sua liberdade. Assim, ao afetar o processo de acesso à informação e,

---

[225] PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You**. New York: The Penguim Press, 2011. p. 63.

[226] EG, Ragnhild; DEMIRKOL TØNNESEN, Özlem Demirko; TENNFJORD, Merete Kolberg. **A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors**. Computers in Human Behavior Reports, v. 9, n. November 2022, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2451958822000872?via%3Dihub> Acesso em ago. 2023. p. 1.

[227] PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You**. New York: The Penguim Press, 2011. p. 89.

[228] PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You**. New York: The Penguim Press, 2011. p. 10.

[229] HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital: desafios para o direito**. – 2. ed. – Rio de Janeiro: Forense, 2022. p. 72.

consequentemente, o pluralismo informativo de fontes, temas e discussões, mais que conectada, a pessoa é vinculada[230] a essa nova ideia de sociedade, pelo que passa a ser manipulada e, por exemplo, a achar que aquele pensamento político é a corrente majoritariamente aceita, que não existem problemas sociais ou que, se existem, não lhe atingem, ou mesmo de que supostamente necessita de ter um determinado bem ou serviço, assim como todas as outras pessoas com as quais têm contato possuem, a abandonar a sua curiosidade[231], dentre outros reflexos e desdobramentos.

[230] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 7.
[231] HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital: desafios para o direito**. – 2. ed. – Rio de Janeiro: Forense, 2022. p. 72.

5 A APLICAÇÃO DA NORMA JURÍDICA PARA A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS VIOLADOS PELA UTILIZAÇÃO DE *DARK PATTERNS* NAS REDES SOCIAIS

A utilização dos sistemas de IA, juntamente com a corrupção do *design* das interfaces de usuário das redes sociais através da aplicação dos *dark patterns*, levanta diversas questões sobre as consequências às pessoas e seus direitos fundamentais. Direitos como a privacidade, a proteção de dados pessoais, a autodeterminação informativa, as liberdades de consciência, expressão, comunicação e de informação, bem como os direitos difusos e coletivos, como aqueles assegurados aos consumidores e, em última instância, a dignidade da pessoa humana como um todo, enfrentam problemas no que tange tanto à sua proteção quanto ao seu exercício nesses novos espaços digitais de interação social. Tendo em vista as transformações em desenvolvimento nas sociedades em decorrência da influência da tecnologia e do uso de suas ferramentas na vida atual, questiona-se de que maneira o Direito, sendo um instrumento de controle social[232], deve intervir para a garantia da devida tutela a tais bens jurídicos frente a essas novas modalidades de violações e riscos, até então desconhecidos, nessas novas dinâmicas de relações digitais.

No tocante à inserção dos *dark patterns* no *design* das interfaces de usuário das redes sociais, nos ordenamentos jurídicos analisados, quais sejam, União Europeia, Brasil e Estados Unidos da América, verifica-se que na atualidade não se dispõe de ferramenta jurídica essencialmente concebida para a finalidade de proibir tais práticas em sua totalidade. Observa-se, em vista disso, uma escassez normativa pela ausência de um documento legal que possa diretamente enfrentar essa problemática. Há, no entanto, algumas legislações voltadas para o âmbito digital, as quais têm alguma aplicação com relação aos *dark patterns*, como no caso do *DSA* e *DMA* no contexto da União Europeia, como será visto adiante. Até o momento, há apenas algumas propostas legislativas que se apresentam como instrumento para regular o desenvolvimento, a implementação e a utilização de sistemas de IA como um todo, bem como seus impactos à vida das pessoas que com eles de alguma forma interagem e, por isso, podem ser identificadas as proibições a tais padrões obscuros.

---

[232] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 2.

No entanto, sabe-se que a ciência jurídica não pode abster-se de sua elementar missão de auxiliar na prevenção, repressão e organização social[233], pelo que com seus já existentes mecanismos legais também deve atuar na defesa dos bens jurídicos, quando envolvidos em um conflito. Deste modo, nesta parte a pesquisa concentrar-se-á sobre as formas encontradas pelas quais o Direito pode intervir para fornecer a devida solução ao problema visualizado da aplicação dos *dark patterns* nas redes sociais. Assim, serão apresentados os meios legais já disponíveis a nível constitucional ou infraconstitucional, bem como as propostas de regulação ainda em discussão nos ordenamentos jurídicos destacados.

5.1 O conflito entre os direitos fundamentais

Por um lado, tem-se que a questão suscitada com a aplicação dos *dark patterns* nas redes sociais provoca reflexões em vários direitos assegurados como fundamentais com relação aos usuários. Por outro lado, porém, no caso das empresas detentoras dessas plataformas, há também os valores norteadores da ordem econômica e das relações comerciais, como as liberdades de iniciativa e de concorrência e a autonomia privada, também reconhecidos como fundamentos do Estado Democrático de Direito. Visualiza-se, em razão disso, uma colisão entre os direitos fundamentais em questão, os quais metaforicamente possuem igual peso normativo, ou seja, mesmo valor ou importância.

Desta forma, para a resolução do conflito revelado entre os direitos fundamentais na situação dos *dark patterns* e a evidente lacuna legislativa nos ordenamentos jurídicos sobre essa matéria, pode-se recorrer à doutrina constitucional para preencher e integrar o Direito[234], pelo que recomenda-se a observância de preceitos da ciência de hermenêutica jurídica, para que seja estabelecido um exercício de interpretação pelo aplicador da norma[235]. Reconhecida a dimensão histórica de tais direitos, a interpretação cumpriria, neste caso, a finalidade de atualização do texto constitucional, para adaptá-lo de acordo com a necessidade que a situação peculiar impõe,

---

[233] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 1.
[234] VARELA, Bartolomeu. **Elementos de Estudo da Teoria da Constituição**. Praia: Universidade de Cabo Verde, 2011. p. 103.
[235] MORAES, Alexandre de. **Direito Constitucional**. – 33. ed. rev. e atual. até a EC n. 95 de 15 de dezembro de 2016. – São Paulo: Atlas, 2017. p. 33.

dadas essas novas demandas sociais que ainda carecem de resposta legal[236], fornecendo-lhe com isso uma solução aparente[237].

Assim, em um primeiro momento, deve-se considerar o princípio da unidade da Constituição, segundo o qual entende-se a Carta Magna como um todo, isto é, um conjunto de normas e princípios de valor constitucional, os quais mantêm um sentido de integração e consonância entre si[238], de modo a evitar possíveis contradições. Isso porque se percebidos em apartado, podem conduzir a soluções distintas e a um provável desacordo[239]. Por conseguinte, deve-se observar o princípio do efeito integrador, pelo qual os dispositivos constitucionais necessitam de serem interpretados à luz da integração social e política, reforçando ainda mais a noção de um sistema unitário de normas.

Por sua vez, segundo o princípio da harmonização ou concordância prática, deve-se colocar os direitos fundamentais em coordenação e combinação entre si, de modo a impedir o sacrifício de algum em relação ao outro na resolução do conflito[240], mas buscar preservar seu núcleo ao máximo possível. A ideia de que não existe hierarquia entre os direitos fundamentais leva, então, ao reconhecimento de limites no âmbito de proteção de cada bem jurídico para que, dadas as circunstâncias de cada caso em concreto, possa nessa ponderação ser estabelecida uma determinada precedência em relação ao outro[241], de acordo com premissas como a igualdade, a razoabilidade e a proporcionalidade[242].

Por isso, enquanto os ordenamentos jurídicos não apresentarem legislações que se destinem a regular a inteligência artificial utilizada para a aplicação dos *dark patterns* nos ambientes digitais, sobretudo na esfera das redes sociais, ou essencialmente tratarem a temática por meio de uma legislação específica para combater tais padrões obscuros, uma das alternativas para uma solução prática para os conflitos entre os direitos fundamentais

---

[236] Segundo a quarta das oito teses básicas de Kirchhof sobre interpretação dos direitos fundamentais. BONAVIDES, Paulo. **Curso de Direito Constitucional**. – 15. ed. São Paulo: Malheiros Editores, 2004. p. 602.
[237] Novelino menciona duas possibilidades de resolução de conflitos entre normas, sendo a primeira intitulada de real, pela qual exclui-se uma das normas envolvidas. Já a segunda seria chamada de aparente, uma vez que utilizaria a interpretação como solução. NOVELINO, Marcelo. **Curso de Direito Constitucional**. – 11. ed. rev., ampl. e atual. – Salvador: Editora Juspodivm, 2016. p. 117.
[238] CANOTILHO, José Joaquim Gomes. **Direito Constitucional**. – 6. ed. rev. Coimbra: Livraria Almedina, 1993. p. 226.
[239] ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. de Virgílio Afonso da Silva. – 2. ed. São Paulo: Malheiros Editores, 2015. p. 96.
[240] NOVELINO, Marcelo. **Curso de Direito Constitucional**. – 11. ed. rev., ampl. e atual. – Salvador: Editora Juspodivm, 2016. P. 136-137; CANOTILHO, José Joaquim Gomes. **Direito Constitucional**. – 6. ed. rev. Coimbra: Livraria Almedina, 1993. p. 228.
[241] ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. de Virgílio Afonso da Silva. – 2. ed. São Paulo: Malheiros Editores, 2015. p. 96.
[242] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: Os Conceitos Fundamentais e a Construção do Novo Modelo**. – 2. ed. São Paulo: Saraiva, 2010. p. 345.

envolvidos será a interpretação da norma constitucional que institui e assegura tais direitos, isso quando houver uma Lei Maior que preveja direitos dessa natureza. Assim, nas hipóteses em que o Poder Judiciário for provocado a manifestar-se diante de uma demanda judicial na qual discute-se algum dos problemas decorrentes dos *dark patterns* nas redes sociais, a interpretação será, em última análise, uma via possível. Por isso, cada situação em concreto pode apresentar peculiaridades e requerer um exercício interpretativo com resultado diverso.

5.2 A utilização das normas já existentes em diferentes ordenamentos jurídicos para combater a aplicação dos *dark patterns* nas redes sociais

Tendo em vista a atual inexistência de lei específica que detenha o papel de atuar no combate a todos os tipos de *dark patterns* inseridos nas redes sociais, não se pode deixar que os problemas decorrentes dessa questão fiquem sem uma solução. Desta forma, pode-se utilizar de outros meios legais já existentes como possíveis alternativas para a tutela dos direitos fundamentais afetados. Assim, tratando-se de dados pessoais, pois como visto são a mercadoria desses modelos de negócio, podem ser aplicadas as normas relativas à proteção desse tipo de informações. Além disso, considerando que o vínculo presente entre o usuário e a plataforma de rede social constitui-se em uma relação de consumo, pode-se também servir das normas de defesa do consumidor para essa finalidade.

Neste sentido, em âmbito europeu, o *General Data Protection Regulation – GDPR*, pode ser utilizado como instrumento legal para o combate aos *dark patterns*, tendo em vista que tal regulação tem vigência sobre todo o ciclo de processamento dos dados pessoais por meios automatizados. Ao passo que as plataformas de redes sociais funcionam com base nos dados de seus usuários coletados de suas contas e perfis pessoais, as disposições normativas do *GDPR* terão aplicabilidade. Assim, desde o momento da inscrição da pessoa como usuário da rede, a sua atividade registrada por meio da utilização, suas comunicações, o exercício de seus direitos fundamentais nesse espaço digital até o fim da relação contratual, na ocasião de exclusão da conta ou perfil, poderá ter a incidência do referido documento legal.

No tocante aos princípios relativos ao tratamento de dados pessoais constantes no artigo 5°, parágrafo 1, alíneas “a”, do *GDPR*, segundo o princípio da licitude, lealdade e transparência, os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente para com seu titular. Pelo princípio da limitação das finalidades, contido na alínea “b”, os dados

devem ser recolhidos para as finalidades determinadas e legítimas, pelo que não podem ser destinados para outros objetivos. Ademais, pelo princípio da minimização dos dados, constante na alínea "c" do mesmo parágrafo, deve tal tratamento seguir uma adequação, pertinência e limitação quanto à necessidade para as finalidades declaradas[243], bem como pelo princípio da responsabilidade, no parágrafo 2, cabe ao responsável por essa atividade de tratamento dos dados a observância dos princípios elencados no aludido texto legal[244]. Além disso, é definido no artigo 4°, parágrafo 11, que o consentimento do titular deve representar uma manifestação de vontade feita de forma livre, específica, informada e explícita, pela qual seja demonstrada a aceitação, por ato inequívoco ou mesmo uma declaração, de que concorda com o tratamento de seus dados pessoais[245].

Em vista disso, no que compete ao consentimento, entende-se pelo artigo 7° que o seu requerimento para coleta e processamento dos dados deve ser informado de maneira inteligível, de fácil acesso e em uma linguagem clara e simples à pessoa titular das informações, o que de certa forma pode ser entendido, para além de outros padrões, como uma proibição ao *dark pattern* de *toying with emotion*, o qual, como já visto, emprega artifícios como a linguagem para provocar abalos afetivos e morais nas pessoas. Além disso, deve ser facilitado tanto o ato de conceder como de retirar a autorização ao tratamento, bem como que deve ser verificado se tal anuência produz efeitos sobre dados os quais não são necessários para a execução dos

---

[243] O artigo 5°, parágrafo 1, alíneas "a", "b" e "c", do *GDPR, in verbis*: *"Article 5. 1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."* EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

[244] O artigo 5°, parágrafo 2, do *GDPR, in verbis*: *"2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."* EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

[245] O artigo 4°, parágrafo 11, do *GDPR, in verbis*: "(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

serviços contratados[246]. Já pela redação do artigo 12°, no que tange à transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares, deve-se fornecer de forma gratuita, transparente, concisa, inteligível e de fácil acesso, todas as informações necessárias sobre o responsável pelo tratamento, utilizando-se de uma linguagem clara e simples, ainda mais se tais informações forem direcionadas a menores de idade.

Por conseguinte, o artigo 15° determina que é direito do titular o acesso às informações pertinentes ao tratamento de seus dados, como com relação à finalidade, as categorias relativas, os destinatários, o prazo previsto de conservação e os critérios para o seu armazenamento. Além disso, constitui também como direito a solicitação ao responsável de atos como a retificação, o apagamento ou a limitação de tal processamento, bem como a possibilidade de reclamação a uma autoridade de controle. Sobre as decisões automatizadas, nas quais são incluídas as técnicas de *profiling*, compreende-se como direito do titular a possibilidade de requerer as informações relativas à importância da definição de perfis, as consequências e até mesmo a lógica de sua constituição.

Já no disposto no artigo 25°, sobre a proteção de dados desde a concepção e por definição, à luz dos princípios elencados no texto legal, devem ser adotadas as medidas técnicas necessárias para garantir a proteção dos dados pessoais tratados, de modo que somente passem por esse processo aqueles entendidos como fundamentais para cada finalidade específica. Assim, devem ser assegurados elementos para a proteção dos direitos do titular, como a autonomia, pela qual deve-se proporcionar a máxima autonomia possível para o titular determinar o uso de seus dados; a interação, para que possam exercer seus direitos, e a expectativa do titular, visto que a atividade de processamento deve correspondê-la.

Para além disso, deve haver também a possibilidade de escolhas ao titular e o equilíbrio de poderes, sempre que possível, na relação entre ele e o responsável pelo tratamento. Por fim,

---

[246] O artigo 7°, do GDPR, *in verbis*: *"Article 7°. 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."* EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

destacam-se também a proibição a fraudes nas informações e opções, de modo a serem fornecidas de maneira clara, objetiva e neutra, evitando-se assim o emprego de linguagem ou *design* manipulador ou enganoso, e a veracidade das informações disponibilizadas, para não induzir as pessoas em erro[247].

Desta forma, vê-se que o *GDPR*, ao impor obrigações sobre a recolha e o tratamento dos dados pessoais, pode ter incidência sobre os *dark patterns*, na medida em que estes relacionam-se com os dados dos usuários das redes sociais. Assim, padrões como o *preselection by default*, *hidden information*, *false hierarchy*, *roach motel* e *forced registration*, mais associados à coleta de dados, podem ser combatidos por meio das normas de proteção constantes no referido documento legal, visto que representam violações a princípios instituídos como da limitação da finalidade, da licitude e da transparência.

Não obstante, como são técnicas pelas quais são desenvolvidas ações sem que o usuário tenha conhecimento, infringem o consentimento, o qual é um direito do titular dos dados. Como visto, esses padrões obscuros funcionam através de diferentes métodos, como a manipulação da linguagem para conseguir a aceitação para a recolha dos dados. Assim, ao distorcer as informações e opções disponíveis, prejudicam a tomada de decisão do usuário sobre os seus dados.

Por sua vez, podem também serem aplicadas as normas do *Digital Services Act - DSA*, legislação europeia do ano de 2022 que propõe-se a ser um pacote regulatório para os serviços digitais, por meio da criação de um ambiente de mercado único com transparência e segurança. É aplicável às plataformas de serviços digitais, consideradas intermediárias entre os consumidores e bens, serviços e conteúdos, classificação da qual as redes sociais fazem parte. Por essa lei, são previstas normas para assegurar a proteção dos consumidores e o respeito aos seus direitos fundamentais, instituindo responsabilidades e obrigações, mas também para promover a inovação, o desenvolvimento e a competitividade no mercado europeu. Conforme já visto anteriormente, nos termos da referida lei, em seu considerando número 67, os *dark patterns* são entendidos como interfaces de plataformas digitais as quais têm o objetivo de ocasionar a distorção ou o prejuízo da capacidade do usuário de fazer escolhas ou tomar

---

[247] Nas orientações apresentadas pelo *European Data Protection Board – EDPB*, foram identificados sete elementos nos princípios de proteção dos dados *by design* e *by default*: (i) *autonomy*; (ii) *interaction*; (iii) *expectation*; (iv) *consumer choice*; (v) *power balance*; (vi) *no deception* e (vii) *truthful*. EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them**. Version 2.0. February, p. 1–74, 2023. Disponível em: <https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> Acesso em set. 2023. p. 13-14.

decisões informadas e autônomas, para persuadi-lo a apresentar determinados comportamentos indesejados, acarretando com isso consequências negativas para si.

Assim sendo, dentre várias obrigações impostas na lei, no artigo 25º do *DSA*, proíbe-se aos fornecedores de plataformas *online* o desenho, a organização e a exploração de suas interfaces de modo a enganar ou manipular os usuários, prejudicando ou distorcendo suas capacidades de tomarem decisões livres e informadas. Apesar de que o referido artigo não menciona expressamente os *dark patterns* ou outra nomenclatura sinônima, pode-se entender que faz referência a tais padrões na medida em que o considerando número 67, citado anteriormente, já definiu claramente, para os termos da lei, o que seriam tais técnicas.

Prevê ainda o mesmo artigo a possibilidade de a Comissão Europeia emitir diretrizes sobre pontos específicos, como acerca do destaque intencional a uma informação ou opção, identificado no caso do *dark pattern* de *false hierarchy*, solicitar reiteradamente uma escolha já decidida pelo usuário por meio da exibição de janelas de notificação que interferem na atividade executada, a exemplo da situação exibida pelas técnicas de *nagging*, bem como na questão do padrão chamado de *roach motel* ou *hard to cancel*, no qual o processo de exclusão e cancelamento do serviço é mais complexo do que a inscrição à plataforma[248]. Ademais, destaca em seu parágrafo 2º que tais proibições não serão aplicáveis às práticas já cobertas pela Diretiva 2005/29/CE, relativa às práticas comerciais desleais, e pelo *GDPR*.

Além disso, sobre a publicidade veiculada nesses espaços digitais, determina-se pelo artigo 26º que as plataformas devem exibir os anúncios publicitários de modo que seja plenamente identificável que uma determinada publicação constitui uma propaganda. Devem, em vista disso, serem sinalizadas as informações referentes a qual pessoa, singular ou coletiva, está sendo representada no anúncio, bem como quem pagou por ele, além de outros dados como sobre os parâmetros avaliados para mostrar tal publicação para o usuário, além da possibilidade de alterá-los. Visualiza-se, assim, uma forma de combater o *dark pattern* chamado de *disguised*

---

[248] O artigo 25º do *DSA*, *in verbis*: *"Article 25º. 1. Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions. 2. The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679. 3. The Commission may issue guidelines on how paragraph 1 applies to specific practices, notably: (a) giving more prominence to certain choices when asking the recipient of the service for a decision; (b) repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience; (c) making the procedure for terminating a service more difficult than subscribing to it."* EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

advertising, pelo qual, como já visto, são inseridos anúncios de publicidade disfarçados entre outras publicações[249].

Sobre a questão dos menores de idade, o artigo 28º impõe a adoção de medidas adequadas e proporcionais, em vista de garantir a tutela de direitos como a privacidade e a sua proteção no ambiente digital. Fica ainda proibida a veiculação de publicidade direcionada feita por meio de técnicas de *profiling*, quando a plataforma tiver conhecimento de que o usuário em questão é um menor de idade[250].

Já no tocante aos termos e condições de uso, conhecidos popularmente como "a lei interna das plataformas", os prestadores dos serviços digitais ficam obrigados a publicar, nas línguas oficiais de todos os países da UE, todas as informações consideradas relevantes sobre sua atividade, incluindo as políticas, os procedimentos, as medidas e os instrumentos utilizados para a moderação de conteúdos, bem como sobre as decisões algorítmicas e seu sistema interno de gestão de reclamações. Para além do idioma do usuário, em vista de possibilitar a sua compreensão, tais informações devem ser apresentadas em linguagem clara, simples e facilmente compreensível, assim como serem disponibilizadas por meios acessíveis, a fim de evitar a aplicação do *dark pattern* de *toying with emotion*, por exemplo[251].

---

[249] O artigo 26º do *DSA*, *in verbis*: *"Article 26º. 1. Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following: (a) that the information is an advertisement, including through prominent markings, which might follow standards pursuant to Article 44; (b) the natural or legal person on whose behalf the advertisement is presented; (c) the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in point (b); (d) meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters."* EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

[250] O artigo 28º do *DSA*, *in verbis*: *"Article 28º.* 1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. 2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor." EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

[251] O artigo 14º do *DSA*, *in verbis*: *"Article 14º. 1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format. 2. Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions. 3. Where an intermediary service*

No que tange às sanções aplicáveis e previstas no *DSA*, nos termos do artigo 52º, fica a cargo dos Estados-Membros a definição das regras relativas às penalidades impostas em caso de descumprimento pelas plataformas *online* às normas do texto legal, devendo serem proporcionais, efetivas e com caráter pedagógico, de modo a desestimular as violações à legislação. Devem os países assegurarem que o valor máximo das multas corresponderá a 6 % (seis por cento) do volume de negócios anual, a nível mundial, no exercício anterior. Nas hipóteses de infrações pelo fornecimento de obrigações incorretas, incompletas ou mesmo enganosas, bem como pela sua não retificação ou ausência de resposta, incorrerão em multa correspondente a 1 % (um por cento) do volume de negócios anual, a nível mundial, no exercício anterior.

Os Países-Membros devem, ainda, garantir que o montante máximo de uma sanção corresponderá a 5 % (cinco por cento) da média do volume de negócios mundial, ou do rendimento diário de uma plataforma de serviços online no seu exercício anterior diário, sendo tal valor calculado a partir da data da decisão que impuser a sanção[252]. Para além das sanções

---

is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand. 4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter. 5. Providers of very large online platforms and of very large online search engines shall provide recipients of services with a concise, easily-accessible and machine-readable summary of the terms and conditions, including the available remedies and redress mechanisms, in clear and unambiguous language. 6. Very large online platforms and very large online search engines within the meaning of Article 33 shall publish their terms and conditions in the official languages of all the Member States in which they offer their services." EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

[252] O artigo 52º do *DSA*, *in verbis*: *"Article 52º. 1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation by providers of intermediary services within their competence and shall take all the necessary measures to ensure that they are implemented in accordance with Article 51. 2. Penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them. 3. Member States shall ensure that the maximum amount of fines that may be imposed for a failure to comply with an obligation laid down in this Regulation shall be 6 % of the annual worldwide turnover of the provider of intermediary services concerned in the preceding financial year. Member States shall ensure that the maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be 1 % of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year. 4. Member States shall ensure that the maximum amount of a periodic penalty payment shall be 5 % of the average daily worldwide turnover or income of the provider of intermediary services concerned in the preceding financial year per day, calculated from the date specified in the decision concerned."* EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

aplicáveis, prevê-se também, no artigo 54º, o direito do usuário a requerer uma indenização à plataforma prestadora de um serviço *online* por perdas e danos decorrentes de uma violação às obrigações dispostas no *DSA*[253].

Desta forma, verifica-se a possibilidade de execução das normas do *DSA* para o combate aos *dark patterns*, uma vez que as redes sociais constituem plataformas prestadoras de serviços digitais. Ao passo que suas regras preveem a vedação de determinadas condutas identificadas em padrões obscuros, pode-se visualizar a cobertura de tais proibições com relação a essas técnicas, visto que a lei proíbe a concepção de uma interface de usuário que apresente os referidos mecanismos. Tendo em vista que a mencionada legislação ainda é recente, pois sua entrada em vigor aconteceu em agosto de 2023, pode ser ainda considerado cedo para observar sua aplicação e efetividade sobre as plataformas de redes sociais, no contexto dos usuários da EU, para resolver tal problemática. O que se sabe é que a maior parte dos padrões obscuros identificados nas arquiteturas das redes sociais ainda continuam a operar suas técnicas sobre as pessoas, causando com isso seus efeitos de distorção da consciência e consequente alteração de seus comportamentos, influenciando negativamente em suas decisões.

Além disso, com os contínuos avanços tecnológicos, há a possibilidade de surgimento de novas formas de *dark patterns*, que podem ser criadas já adaptadas às normas legais do *DSA*, de modo que não sejam cobertas por elas, expondo de outro modo os usuários e seus direitos fundamentais. Para mais, considerando que as normas do *DSA* não tem aplicabilidade sobre as micro e pequenas empresas, em razão de evitar encargos desproporcionais, pode haver, ainda, a possibilidade de os padrões obscuros serem inseridos em redes sociais consideradas de pequeno porte, isto é, aquelas acessíveis e destinadas para um determinado público, estando seus usuários vulneráveis a possíveis manipulações e interferências no *design* de tais plataformas.

Há também a possibilidade de aplicação do *Digital Markets Act - DMA*, legislação da União Europeia do ano de 2022, cuja finalidade é regular o mercado digital no âmbito europeu, a fim de estabelecer um quadro normativo destinado às empresas entendidas como controladoras de acesso que prestam serviços em plataformas online, dentre as quais estão as

---

[253] O artigo 54º do *DSA*, *in verbis*: *"Article 54º. Recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation."* EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

redes sociais[254]. A exemplo de outros documentos legais europeus como os já mencionados *GDPR* e o *DSA*, também demonstra preocupação com o livre consentimento informado do consumidor sobre a coleta e processamento de seus dados pessoais, bem como acerca da tomada de decisão de suas ações dentro da plataforma.

Embora a maioria das determinações que têm ligação com a questão dos *dark patterns* estão presentes no *DMA* em seus considerandos, os quais não possuem força normativa, entende-se que são de fundamental importância, visto que contribuem não somente para a afirmação do propósito da legislação, como também para o esclarecimento de possíveis questões na sua fase de interpretação e aplicação. Além disso, diferente das normas do *DSA*, nas quais esses padrões foram expressamente mencionados, não há citação a este nem a outro termo sinônimo em seu texto, mas é possível compreender quando a lei está referindo-se a tais técnicas. Assim, diz em seu considerando número 37, que os controladores de acesso não poderão desenhar, organizar nem mesmo operar suas interfaces de usuário para enganar, manipular ou de outro modo promover a distorção e o prejuízo da capacidade do utilizador de fornecer livremente seu consentimento, devendo ainda ser facilitado tanto concedê-lo como retirá-lo[255].

Nesse mesmo considerando, determina-se que os controladores não poderão requerer o consentimento para a mesma finalidade de tratamento dos dados mais do que uma vez por ano, quando o usuário já tenha recusado ou mesmo retirado seu aceite, o que, em outras palavras, pode ser entendido como uma proibição ao *dark pattern* identificado como *nagging*. Por sua vez, nos termos do considerando número 49, deve-se permitir ao usuário a fácil alteração das configurações padrões em todos os formatos em que o serviço é oferecido, sempre que tais ajustes favoreçam as opções desejadas pelo sistema, podendo assim ser verificado o

---

[254] EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

[255] O Considerando n. 37, *in verbis*: *"[...] Lastly, it should be as easy to withdraw consent as to give it. Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent. In particular, gatekeepers should not be allowed to prompt end users more than once a year to give consent for the same processing purpose in respect of which they initially did not give consent or withdrew their consent. This Regulation is without prejudice to Regulation (EU) 2016/679, including its enforcement framework, which remains fully applicable with respect to any claims by data subjects relating to an infringement of their rights under that Regulation."* EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

mecanismo obscuro chamado de *preselection by default*[256]. Já no considerando número 63, em vista de preservar a liberdade de escolha do usuário, deve ser assegurada a possibilidade de encerramento da relação contratual entre o consumidor e o prestador do serviço *online* da plataforma, sendo proibido tornar desnecessariamente difícil o processo de cancelamento de uma assinatura ou exclusão de conta ou perfil, o que pode ser entendido como uma vedação ao padrão chamado de *roach motel* ou *hard to cancel*[257].

Sobre as vedações em relação à interface de usuário, destaca-se no seu artigo 13º a proibição a comportamentos que violem as disposições legais do *DMA*, dentre as quais está desenhar as suas interfaces de usuário de maneira a subverter ou prejudicar a autonomia, a tomada de decisão ou a escolha do usuário a fim de contornar o devido cumprimento de tais obrigações[258]. Determina a lei, ainda, a vedação à apresentação de escolhas de forma não neutra,

---

[256] O Considerando n. 49, *in verbis*: *"[...] Gatekeepers should also allow end users to easily change the default settings on the operating system, virtual assistant and web browser when those default settings favour their own software applications and services. This includes prompting a choice screen, at the moment of the users' first use of an online search engine, virtual assistant or web browser of the gatekeeper listed in the designation decision, allowing end users to select an alternative default service when the operating system of the gatekeeper directs end users to those online search engine, virtual assistant or web browser and when the virtual assistant or the web browser of the gatekeeper direct the user to the online search engine listed in the designation decision."* EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

[257] O Considerando n. 63, *in verbis*: *"Gatekeepers can hamper the ability of business users and end users to unsubscribe from a core platform service that they have previously subscribed to. Therefore, rules should be established to avoid a situation in which gatekeepers undermine the rights of business users and end users to freely choose which core platform service they use. To safeguard free choice of business users and end users, a gatekeeper should not be allowed to make it unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service. Closing an account or un-subscribing should not be made be more complicated than opening an account or subscribing to the same service. Gatekeepers should not demand additional fees when terminating contracts with their end users or business users. Gatekeepers should ensure that the conditions for terminating contracts are always proportionate and can be exercised without undue difficulty by end users, such as, for example, in relation to the reasons for termination, the notice period, or the form of such termination. This is without prejudice to national legislation applicable in accordance with the Union law laying down rights and obligations concerning conditions of termination of provision of core platform services by end users."* EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

[258] O artigo 13º, parágrafos 4 e 6, *in verbis*: *"4. The gatekeeper shall not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design. 6. The gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof."* EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

o que pode ser verificado nos *dark patterns* identificados como *false hierarchy*, *hidden information* ou *preselection by default*, os quais, como já relatado, buscam, de maneiras diferentes, influenciar negativamente as escolhas do usuário, para levá-lo a aceitar a opção desejada pelo sistema.

No tocante às sanções pelo descumprimento da lei, prevê-se no artigo 30º a aplicação de multa em um valor não superior a 10 % (dez por cento) do volume de negócios anual a nível mundial no exercício anterior, quando for verificado que o controlador, por negligência ou deliberadamente, violou suas obrigações legais. Há também a previsão de multa em um valor não superior a 20% (vinte por cento) do volume de negócios anual a nível mundial no exercício anterior, quando houver reincidência nas violações[259].

No âmbito da União Europeia, observa-se mais uma vez a possibilidade de combater os *dark patterns* inseridos nas plataformas digitais por meio da aplicação de legislações já existentes, a exemplo das mencionadas leis do *GDPR*, *DSA* e *DMA*, na medida em que seus escopos de atuação têm alguma relação com tais padrões obscuros, como sobre o consentimento e a proteção de dados pessoais. Embora essas leis até possam ser empregadas sobre tal questão, podem não ser medidas suficientemente satisfatórias para combatê-los, já que podem não incidir sobre outros tipos de técnicas, como no caso dos padrões de *infinite scroll*, *autoplay design*, *activity messages* e *intermediate currency*, tão danosos aos direitos fundamentais dos usuários como outros mencionados e que também necessitam de regulação. Além disso, como visto, considerando que o *DSA* e o *DMA* são leis muito recentes, pode ainda não ser possível avaliar sua aplicação e efetividade para resolver esse problema.

No tocante às leis existentes no contexto do Brasil e seu ordenamento jurídico, assim como no caso da União Europeia e seu *GDPR*, podem ser aplicáveis as normas constantes na Lei Geral de Proteção de Dados Pessoais – LGPD, ao passo que promovem a proteção dos dados pessoais das pessoas, a autodeterminação informativa e o livre desenvolvimento da personalidade, dentre outros direitos fundamentais. Isso porque, como já visto, as redes sociais

---

[259] O artigo 30º, parágrafo 1, alínea "a" e parágrafo 2, *in verbis*: *"1. In the non-compliance decision, the Commission may impose on a gatekeeper fines not exceeding 10 % of its total worldwide turnover in the preceding financial year where it finds that the gatekeeper, intentionally or negligently, fails to comply with: (a) any of the obligations laid down in Articles 5, 6 and 7; 2. Notwithstanding paragraph 1 of this Article, in the non-compliance decision the Commission may impose on a gatekeeper fines up to 20 % of its total worldwide turnover in the preceding financial year where it finds that a gatekeeper has committed the same or a similar infringement of an obligation laid down in Article 5, 6 or 7 in relation to the same core platform service as it was found to have committed in a non-compliance decision adopted in the 8 preceding years."* EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

e os *dark patterns* operam utilizando-se dos dados pessoais dos usuários, bem como manipulando seus consentimentos para coletar e processar tais informações[260].

Sendo assim, nos termos de seu artigo 6º, acerca dos princípios regentes para as atividades de tratamento de dados, para além da boa-fé, devem ser observados os princípios da finalidade (inciso I), pelo qual determina-se que o tratamento tenha objetivos legítimos, específicos, explícitos e informados ao titular, impedidas quaisquer possibilidades posteriores de tratamento para fins incompatíveis a tais preceitos. Ademais, pelo princípio da adequação (inciso II), deve haver compatibilidade entre o tratamento, o contexto e as finalidades informadas ao titular. Já pelo princípio da necessidade (inciso III), o tratamento deve ser limitado ao mínimo necessário, com proporcionalidade à sua finalidade e, pelo princípio da transparência, é garantido ao titular o fornecimento de informações com clareza, precisão e facilmente acessíveis sobre o tratamento, sua realização e sobre os operadores e controladores dos dados. Ainda, pelo princípio da não-discriminação (inciso IX), os dados não podem ser tratados para fins discriminatórios, ilícitos ou mesmo abusivos[261].

Além disso, segundo o artigo 7º, inciso I, da LGPD, o tratamento dos dados pessoais só pode ser realizado com o consentimento do seu titular, sendo que para o compartilhamento dessas informações com outros controladores deve ser requerido um consentimento específico. O consentimento, deve, ainda, nos termos do artigo 8º, ser fornecido por escrito ou por outra forma que demonstre claramente a vontade do titular, sendo vedado expressamente o tratamento feito por meio de vício de consentimento e podendo também ser revogado a qualquer tempo por manifestação expressa. No caso de menores de idade, tal aceitação deve ser dada por pelo menos um de seus pais ou por seu responsável legal, bem como que as informações relativas ao tratamento dos dados devem ser fornecidas em linguagem simples, clara e acessível,

---

[260] BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

[261] O artigo 6º, da LGPD, incisos I, II, III e IV, *in verbis*: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais." BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

considerando os aspectos físico-motores, perceptivos, sensoriais, intelectuais e mentais desses usuários[262].

Sobre possíveis descumprimentos às disposições legais da LGPD, o controlador ou o operador é obrigado, nos termos do artigo 42, *caput*, a reparar os danos, seja moral, patrimonial, individual ou coletivo, causados em razão do tratamento dos dados[263]. Além disso, podem ser aplicadas aos agentes de tratamento as sanções administrativas relativas a infrações às normas legais, previstas no artigo 52 da LGPD. Para além de advertência, com estipulação de prazo para medidas de adequação, pode ser arbitrado o pagamento de multa simples de até 2 % (dois por cento) do faturamento no último exercício da pessoa jurídica em questão, seja uma empresa, grupo ou conglomerado, com o limite de R$ 50.000.000,00 (cinquenta milhões de reais) por cada violação, além de multa diária, observado o referido limite, dentre outras penalidades[264].

Segundo o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, publicado no ano de 2023 pela Autoridade Nacional de Proteção de Dados – ANPD, autoridade responsável por zelar, aplicar e fiscalizar o cumprimento das normas da LGPD no Brasil, o valor arbitrado na multa simples será acrescido em 10 % (dez por cento) até o limite de 40 % (quarenta por cento) para cada caso de reincidência específica, isto é, quando houver violação pelo mesmo infrator ao mesmo dispositivo legal em um período de cinco anos entre o trânsito em julgado do processo administrativo e a nova infração. Nas situações de reincidência considerada genérica, ou seja, quando houver a repetição de uma mesma infração, independente do dispositivo normativo ou regulamentar violado, o acréscimo será de 5 % (cinco por cento) até o limite de 20 % (vinte por cento). Já para cada medida de orientação ou preventiva desrespeitada na fiscalização ou no procedimento que antecedeu o processo administrativo, 20

---

[262] O artigo 7º, inciso I, da LGPD, *in verbis:* "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular." BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

[263] O artigo 42, *caput*, da LGPD, *in verbis:* "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo." BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

[264] O artigo 52, *caput*, incisos I, II, III, da LGPD, *in verbis*: "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II." BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

% (vinte por cento) até o limite de 80 % (oitenta por cento) e para cada medida corretiva descumprida, 30 % (trinta por cento) até o limite de 90 % (noventa por cento)[265].

Desta forma, por meio de um exercício de interpretação normativa, verifica-se uma estreita possibilidade de aplicação das disposições legais da LGPD, isto é, quando um padrão obscuro descumprir tais determinações acerca da proteção de dados pessoais do usuário de uma rede social, bem como sobre o tratamento de tais informações sem o seu consentimento ou, ainda, quando este foi fornecido com algum vício. Assim, nas hipóteses em que um *dark pattern* de algum modo força o usuário a fornecer essa autorização, pode-se de certa forma combater tal prática através do referido documento legal. Observa-se, contudo, que a LGPD não representa medida razoavelmente eficaz para essa finalidade, pois apenas teria alguma cobertura sobre as técnicas obscuras que aproveitam-se dos dados pessoais dos usuários e corrompem o consentimento dado para o seu tratamento, deixando de abranger outros tipos de padrões que afetam outros direitos fundamentais.

Por outro lado, considerando que o usuário de uma rede social é entendido como consumidor desse serviço digital, podem também ser aplicadas as normas dispostas no Código de Defesa do Consumidor – CDC, por meio de interpretações extensivas para adaptá-las às situações peculiares envolvendo os usuários e as plataformas de redes sociais. Desta forma, seu artigo 4º, inciso III, determina como princípio a ser observado para a harmonia nas relações de consumo a boa-fé e o equilíbrio entre consumidor e fornecedor[266]. Além disso, compreende em seu artigo 6º como direitos básicos a informação adequada e clara a respeito dos produtos e

---

[265] O artigo 12, da Resolução de Dosimetria da ANPD, *in verbis*: "Art. 12. O valor da multa simples será acrescido nos percentuais abaixo, caso incidam as seguintes circunstâncias agravantes: I - 10% (dez por cento) para cada caso de reincidência específica, até o limite de 40% (quarenta por cento); II - 5% (cinco por cento) para cada caso de reincidência genérica, até o limite de 20% (vinte por cento); III - 20% (vinte por cento) para cada medida de orientação ou preventiva descumprida no processo de fiscalização ou do procedimento preparatório que precedeu o processo administrativo sancionador, até o limite de 80% (oitenta por cento); e IV - 30% (trinta por cento) para cada medida corretiva descumprida, até o limite de 90% (noventa por cento). § 1º Na hipótese de incidência de mais de um dos incisos deste artigo, deverão ser somados os percentuais relativos a cada fator." DIÁRIO OFICIAL DA UNIÃO. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados. ed. 39., seção 1, p. 59. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf> Acesso em set. 2023.

[266] O artigo 4º, inciso III, do CDC, *in verbis*: "Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

serviços (inciso III), devendo ainda ser acessível à pessoa com deficiência, conforme o parágrafo único desse artigo. Ademais, é garantida a proteção contra a publicidade considerada enganosa e abusiva, bem como contra meios desleais e coercitivos e contra práticas e cláusulas contratuais abusivas (inciso IV), as quais também não podem sofrer modificações que signifiquem prestações desproporcionais ou excessivamente onerosas (inciso V)[267].

A respeito da publicidade, segundo o artigo 31, *caput*, a oferta e apresentação de produtos e serviços deve ser feita com informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre todos seus atributos e informações importantes[268]. Outrossim, deve também ser facilmente identificada, sendo proibida a publicidade enganosa e abusiva, nos termos dos artigos 36, *caput* e 37. É enganosa quando constitui informação inteira ou parcialmente falsa, ou por outro modo ou omissão é capaz de levar o consumidor a erro sobre qualquer dado relativo ao produto ou serviço. Por sua vez, é abusiva quando é discriminatória, incita a violência ou, dentre outros fatores, é capaz de influenciar o comportamento do consumidor de forma prejudicial ou perigosa à sua saúde ou segurança[269]. Neste caso, pode ser entendido como publicidade enganosa e abusiva aquela veiculada por meio do *dark pattern* identificado como *disguised advertising*, pelo qual, como já visto, são inseridos anúncios de publicidade sem a correta e clara indicação de que constitui uma propaganda.

---

[267] O artigo 6º, incisos III, IV e V, do CDC, *in verbis*: "Art. 6º São direitos básicos do consumidor: III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

[268] O artigo 31, *caput*, do CDC, *in verbis*: "Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

[269] Os artigos 36, *caput* e 37, do CDC, *in verbis*: "Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal. Art. 37. É proibida toda publicidade enganosa ou abusiva. § 1° É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços. § 2° É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança. § 3° Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

Compreende-se como prática abusiva, à luz do artigo 39 do CDC, dentre outras questões, aproveitar-se da fraqueza ou ignorância do consumidor, considerando fatores como sua saúde, faixa etária, conhecimento ou condição social, para forçar-lhe a adquirir produtos ou serviços[270]. Neste caso, pode-se buscar interpretar de forma extensiva tal artigo para alcançar a questão dos *dark patterns*, na medida em que tais padrões aproveitam-se dessas condições para tirar proveito dos usuários e impor condições desnecessárias, ou mesmo subverter o consentimento para recolha e processamento de seus dados pessoais. Pode também ser entendida como prática abusiva exigir vantagem manifestamente excessiva nas hipóteses em que, por meio da aplicação de *dark patterns*, é feito o requerimento de consentimento à coleta e tratamento dos dados pessoais do usuário para além do necessário à finalidade declarada, ou mesmo quando tal processamento é realizado sem a aceitação expressa do usuário[271].

Ademais, são entendidas como cláusulas contratuais abusivas, sendo nulas de pleno direito, aquelas que impossibilitem, exonerem ou atenuem as responsabilidades do fornecedor, ou signifiquem a renúncia de direitos do consumidor, bem como as que autorizem a alteração unilateral dos termos contratuais. Tais disposições também podem ser aplicadas quando são referenciadas aos termos e condições de serviço das redes sociais, visto que são uma espécie de contrato de fornecimento de serviços entre o consumidor e a plataforma.

Dentre as sanções administrativas previstas no CDC, estão a aplicação de multa, a suspensão do fornecimento de serviços e produtos e a suspensão temporária da atividade, nos termos do artigo 56, incisos I, VI e VII[272]. Já no que tange às infrações penais, constitui crime contra as relações de consumo, segundo o artigo 67, fazer ou promover publicidade enganosa ou abusiva, sob pena de detenção de três meses a um ano, além de multa. É também crime, à luz do artigo 68, fazer ou promover publicidade que é capaz de induzir o consumidor a adotar comportamento prejudicial ou perigoso à sua saúde ou segurança, com pena de detenção de seis

---

[270] O artigo 39, *caput* e inciso IV, do CDC, *in verbis*: "Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: IV - prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

[271] O artigo 39, inciso V, do CDC, *in verbis*: "V - exigir do consumidor vantagem manifestamente excessiva." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

[272] O artigo 56, *caput* e incisos I, VI e VII, do CDC, *in verbis*: "Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas: I - multa; IV - cassação do registro do produto junto ao órgão competente; VII - suspensão temporária de atividade." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

meses a dois anos e multa. Constitui circunstância agravante o fato de o crime ocasionar grave dano individual ou coletivo[273].

Desta forma, verifica-se que, por intermédio de um exercício de interpretação extensiva, podem ser aplicáveis as disposições normativas do CDC, visto que fornecem proteção aos direitos dos consumidores, o que, no caso das redes sociais, são seus usuários. Contudo, frente a essas novas situações peculiares criadas na relação entre o usuário e a plataforma e as novas formas de violações a direitos fundamentais provocadas pela inserção dos *dark patterns* nesses espaços digitais, considera-se que tanto o CDC como a LGPD não representam medida suficientemente efetiva para essa finalidade, pelo que, com a análise do atual estado do ordenamento jurídico brasileiro, mostra-se ser necessária nova legislação para que possa garantir a justa proteção aos direitos fundamentais dos usuários de plataformas digitais, sobretudo as redes sociais, de modo a proibir a utilização de tais mecanismos prejudiciais.

Por sua vez, no âmbito dos Estados Unidos da América, não se observou a existência de legislação específica para o tratamento da problemática dos *dark patterns* em âmbito federal, tendo, no entanto, algumas legislações estaduais que tratam o tema no que diz respeito à proteção de dados pessoais e dos direitos dos consumidores. Assim, podem ser aplicáveis as normas da *Federal Trade Commission Act*, legislação com o propósito de regular as atividades da referida agência reguladora no país. Embora seu texto seja anterior até mesmo a própria IA, sofreu alterações por meio de uma emenda em 2006, conhecida como *FTC Safe Web*, para incluir disposições atualizadas a fim de fortalecer a proteção dos direitos dos consumidores estadunidenses. Conforme já visto anteriormente, para a *FTC* os *dark patterns* são entendidos como modalidades de atos ou práticas desleais ou enganosas, as quais aproveitam-se de vieses cognitivos dos consumidores para controlar seus comportamentos ou atrasar o acesso à informação para tomar decisões[274].

Assim, nos termos da referida lei, nos casos de violação por práticas desleais pode ser arbitrada uma penalidade civil em um importe de não mais que US$ 10.000,00 (dez mil dólares)

---

[273] O artigo 67, *caput* e 68, *caput*, do CDC, *in verbis*: "Art. 67. Fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva. Pena - Detenção de três meses a um ano e multa. Art. 68. Fazer ou promover publicidade que sabe ou deveria saber ser capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa a sua saúde ou segurança. Pena - Detenção de seis meses a dois anos e multa." BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

[274] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. United States of America, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-FINAL.pdf> Acesso em jun. 2023. p. 2.

por cada infração apurada. Já nas hipóteses de propagandas consideradas enganosas, isto é, aquelas veiculadas com a finalidade de ludibriar ou enganar o consumidor, incorre no pagamento de multa não superior a US$ 5.000,00 (cinco mil dólares) ou prisão não superior a seis meses, ou ainda, as duas penalidades juntas. Se tal situação for uma reincidência, a multa poderá ser em um valor de até US$ 10.000,00 (dez mil dólares), ou de prisão de até um ano, ou mesmo as duas penalidades em conjunto[275].

Desta forma, verifica-se a possibilidade de aplicação da referida lei para o combate aos *dark patterns*, uma vez que, embora seja um documento legal antigo, ainda possui efetividade. Conforme mencionado anteriormente, a *FTC* realizou um *workshop* sobre essa temática no qual discutiu os impactos desses padrões obscuros nas relações de consumo e esclareceu os esforços que têm feito para coibi-los, pelo que destacou algumas legislações a nível estadual que podem ser aplicadas, em conjunto com as normas do *FTC Act*, para essa finalidade[276]. Já há, inclusive, a atuação da agência no combate aos *dark patterns* inseridos em outros contextos, como em sites de compras e jogos online, mas não especificamente em face das redes sociais. Além disso, como será visto adiante, as disposições normativas do *FTC Act*, no tocante às sanções, são invocadas por legislações estaduais que tratam de questões envolvendo a privacidade e outros direitos dos consumidores, também aplicáveis à situação de tais mecanismos obscuros.

Não obstante, no ano de 2022 foi aprovada uma lei federal chamada *Algorithmic Accountability Act*, pela qual impõe-se responsabilidade e deveres de transparência sobre as decisões algorítmicas, além de promover a proteção dos consumidores, dos dados pessoais e dos direitos fundamentais como um todo. Embora não mencione expressamente o termo *dark patterns* ou outro sinônimo, na sua seção 9 sobre a aplicação da lei, entende que uma violação por atos ou práticas desleais e enganosas nas decisões automatizadas deve ser tratada do modo como o *FTC Act* enfrenta tal situação, aplicando-se as mesmas penalidades já mencionadas.

Tendo em vista que na subdivisão interna dos Estados Unidos, seus estados possuem alguns poderes e relativa autonomia em relação ao governo federal, há algumas legislações estaduais nas quais a presente temática dos padrões obscuros é de alguma forma enfrentada. Menciona-se, por exemplo, que no estado da Califórnia há uma lei, do ano de 2018, chamada

---

[275] FEDERAL TRADE COMMISSION. **Federal Trade Commission Act**. United States of America, 1914. Disponível em: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim> Acesso em set. 2023.

[276] FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. United States of America, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800_Dark_Patterns_Report_9.14.2022_-FINAL.pdf> Acesso em jun. 2023. p. 20.

de *California Privacy Rights Act – CPRA*, na qual os *dark patterns* são entendidos, nos termos de sua seção 1798.140, na subdivisão (l) sobre as definições legais, como sendo uma interface de usuário projetada ou manipulada para produzir como efeito a subversão ou prejuízo da autonomia do usuário, influenciando negativamente sua tomada de decisão ou escolhas[277].

Na mesma referida seção, na subdivisão (h), a lei define o que viria a ser entendido como consentimento, sendo qualquer manifestação de vontade fornecida pelo consumidor ou por seu responsável de forma livre, informada e inequívoca, a qual signifique a sua anuência ao processamento de seus dados pessoais para uma determinada e específica finalidade. Ainda, salienta que a mera aceitação dos termos e condições de uso gerais ou de outro semelhante documento não será considerada como consentimento para o tratamento de informações pessoais em conjunto com outros tipos de informações. Além disso, destaca que um consentimento obtido por meio do uso de um *dark pattern* não será aceito como tal, nem mesmo ações como passar o cursor ou mouse sobre uma opção, silenciar, pausar ou até fechar um determinado conteúdo.[278] Explicita ainda a lei, em sua seção 1798.185, subdivisão (a) (20) (C) (iii), que passará pela adoção de futuras regulações para estabelecer regras e procedimentos em um prazo determinado para tópicos específicos, como a certificação de que qualquer *link* para uma página da *web* não terá em seu conteúdo o uso de *dark patterns*[279].

---

[277] Segundo a seção 1798.140, subdivisão (l), *in verbis*: *"'"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."* CALIFORNIA LEGISLATIVE INFORMATION. **Civil Code – CIV. Title 1.81.5. California Consumer Privacy Act of 2018**. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> Acesso em set. 2023.

[278] Nos termos da seção 1798.140, subdivisão (h), *in verbis*: *"(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."* CALIFORNIA LEGISLATIVE INFORMATION. **Civil Code – CIV. Title 1.81.5. California Consumer Privacy Act of 2018**. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> Acesso em set. 2023.

[279] De acordo com a seção 1798.185, subdivisão (a) (20) (C) (iii), *in verbis*: *"(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: […] (20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should: […] (C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in: […] (iii) Does not make use of any dark patterns."* CALIFORNIA LEGISLATIVE INFORMATION. **Civil Code – CIV. Title 1.81.5. California Consumer Privacy Act of 2018**. Disponível em:

Por fim, os descumprimentos às normas do referido texto legal serão passíveis de penalidades, dentre as quais está o pagamento de multa administrativa no importe de até US$ 2.500,00 (dois mil e quinhentos dólares) por cada infração verificada, ou de até US$ 7.500,00 (sete mil e quinhentos dólares) no caso de uma violação intencional envolvendo dados pessoais de consumidores menores de idade. Há ainda a previsão de responsabilidade solidária entre os causadores de tais atos[280].

Menciona-se também a legislação do estado do Colorado, conhecida como *Colorado Privacy Act*, apresentada no ano de 2021, para tratar do direito fundamental à privacidade como uma liberdade individual de seus cidadãos, o que inclui também a proteção de seus dados pessoais. Assim, a lei aborda a questão dos *dark patterns* à medida em que relacionam-se com o consentimento no processamento de dados pessoais. Em sua seção 6-1-1303 (9), no tocante às definições, compreende tais padrões obscuros como sendo uma interface de usuário desenhada ou manipulada para apresentar como efeito a distorção ou o prejuízo da autonomia da pessoa, sua tomada de decisão ou escolha[281].

Desta forma, para os fins da referida lei, entende-se que não constitui consentimento para o tratamento dos dados pessoais do usuário a aceitação obtida por meio dos *dark patterns*[282]. Ademais, determina-se a proibição à adoção de mecanismos de definição padrão

---

<https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> Acesso em set. 2023.

[280] De acordo com a seção 1798, subdivisões (a) (2) e (b), *in verbis*: *"(a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following: […] (2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating. (b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable."* CALIFORNIA LEGISLATIVE INFORMATION. **Civil Code – CIV. Title 1.81.5. California Consumer Privacy Act of 2018**. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> Acesso em set. 2023.

[281] A seção 6-1-1303 (9), *in verbis*: *"As used in this part 13, unless the context otherwise requires: (9) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."* GENERAL ASSEMBLY OF THE STATE OF COLORADO. **Colorado Privacy Act**. Senate Bill 21-190, 2021. Disponível em: <https://legiscan.com/CO/text/SB190/2021> Acesso em set. 2023.

[282] A seção 6-1-1303 (5) (c), *in verbis*: *"Consent" means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data. The following does not constitute consent: (c) Agreement obtained through dark patterns."* GENERAL ASSEMBLY OF THE STATE OF COLORADO. **Colorado Privacy Act**. Senate Bill 21-190, 2021. Disponível em: <https://legiscan.com/CO/text/SB190/2021> Acesso em set. 2023.

acerca do processamento dos dados, mas de meios que representem a escolha livre, afirmativa e inequívoca do consumidor titular de tais informações[283]. Segundo o que dispõe o texto legal, sua aplicação é de competência do Procurador Geral do Estado do Colorado e das Procuradorias Distritais, sendo que o descumprimento à lei será tratado como uma prática comercial enganosa ou desleal e seu infrator incorrerá em penalidades de até US$ 20.000,00 (vinte mil dólares) por violação e até a US$ 500.000,00 (quinhentos mil dólares) por uma série de violações.

Por tudo isso, verifica-se nos ordenamentos jurídicos analisados que, embora as legislações já existente, como leis de proteção de dados pessoais e de direito do consumidor, possam de alguma forma serem aplicadas por meio de interpretações extensivas para proteger os direitos fundamentais expostos à problemática dos *dark patterns*, não se apresentam como ferramenta eficientes em sua totalidade para essa finalidade. Apesar de que no âmbito da União Europeia já há o *DSA* e o *DMA*, sendo duas novas estruturas regulatórias destinadas para as peculiaridades do ambiente digital, por serem medidas recentes, ainda não é possível avaliar sua efetividade sobre os *dark patterns* e todos os seus diferentes tipos. Contudo, podem ser considerados como duas importantes iniciativas para tal propósito.

Apurou-se que no Brasil a LGPD, lei para a proteção de dados pessoais, pode ter alguma aplicação para combater determinados tipos de padrões, mas não fornece cobertura a todos os tipos já existentes, limitando-se àqueles relacionados aos dados pessoais dos usuários. Já o CDC, a legislação acerca dos direitos dos consumidores, também pode até ter alguma aplicação, mas carecerá de um exercício exaustivo de interpretação para alinhar sua proteção ao combate de tais técnicas obscuras, sendo, portanto, recomendada a elaboração de um novo texto legal para enfrentar a questão dos *dark patterns* e garantir a proteção dos direitos fundamentais por eles violados.

Observa-se que, no contexto dos Estados Unidos da América, a cobertura legal apta a combater os *dark patterns* resultará de como cada unidade estadual enfrentará o tema, uma vez que ainda não há lei geral a nível federal com esse propósito. Assim sendo, a depender da abordagem dada por cada legislação, poderão ser apresentadas diversas perspectivas, interpretações e penalidades à questão das práticas obscuras no âmbito digital, estando incluídas as redes sociais, o que pode abrir espaço à insegurança jurídica se tais legislações não mantiverem uma harmonia em suas normas para a proteção dos direitos fundamentais

[283] A seção 6-1-1313 (2) (c), *in verbis*: *"(c) Not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data pursuant to section 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B)."* GENERAL ASSEMBLY OF THE STATE OF COLORADO. **Colorado Privacy Act**. Senate Bill 21-190, 2021. Disponível em: <https://legiscan.com/CO/text/SB190/2021> Acesso em set. 2023.

envolvidos. Desta forma, os usuários identificados como consumidores de uma mesma plataforma de rede social podem ter diferentes estruturas digitais, dependendo do tipo de obrigação que a legislação local impor, bem como resoluções diversas quanto ao enfrentamento de problemas semelhantes em estados diferentes.

5.3 As propostas de regulação jurídica da inteligência artificial em diferentes ordenamentos jurídicos

Considerando as transformações tecnológicas que as aplicações da IA têm ocasionado em diferentes setores e níveis da sociedade, imprescindível faz-se a chamada ao Direito para atuar na intervenção que tem-se mostrado ser medida necessária a fim de regulamentar o desenvolvimento, a implementação, a pesquisa e o uso de seus mais variados sistemas. Isso porque sem o estabelecimento de parâmetros legais para fornecer a resposta adequada para solucionar os novos riscos e problemas enfrentados, pode-se gerar insegurança jurídica e até mesmo acarretar o desabrigo de bens juridicamente e historicamente já tutelados.

Como se sabe, nos ordenamentos jurídicos analisados, até presente o momento não foi verificada a existência de lei cujo papel seja abordar especificamente a situação problemática criada pelos *dark patterns* nas redes sociais. Na medida em que as plataformas desse modelo de negócio funcionam utilizando-se de sistemas de IA e seus algoritmos, a exemplo dos métodos de *machine learning*, a alternativa que apresenta-se como viável até então é tratar essa temática por meio da regulação da inteligência artificial de uma forma geral.

Desta forma, para o desenvolvimento de um documento legal de governança da IA que possa então promover a confiança, a transparência e a responsabilidade desses sistemas, bem como cumprir a finalidade tanto de estimular a inovação tecnológica e científica, quanto de garantir a proteção dos direitos e liberdades fundamentais envolvidos, recomenda-se a sua construção com base em quatro atributos considerados essenciais, quais sejam, a integridade, a explicabilidade, a equidade e a resiliência. Sendo assim, pela integridade requer-se a adequação dos sistemas algoritmos e a validade tanto dos dados usados como de sua própria utilização em si; a explicabilidade, pela qual impõe-se a transparência no processo de tomada de decisão algorítmica. Já pelo fator da equidade devem ser determinados padrões éticos e livres de vieses

e preconceitos e, por sua vez, pela resiliência requerem-se uma robustez técnica, além de conformidade e resistência contra problemas e elementos externos[284].

Em vista disso, diante das transformações sociais decorrentes dos avanços tecnológicos, nos últimos anos tem-se verificado que diferentes países estão buscando trabalhar a temática da IA em seus contextos legais, de modo a confeccionar, com a articulação tanto de atores estatais e privados como de associações e entidades da sociedade civil, uma legislação que tenha o papel de regular a IA. Verifica-se, assim, que além de uma disputa pela liderança no desenvolvimento tecnológico da área, os países pretendem alcançar também uma posição de vanguarda quanto a uma proposta regulatória para a IA que possa ter impactos a nível nacional, regional e até mesmo global[285].

Neste sentido, a União Europeia apresentou no ano de 2021 o chamado *Artificial Intelligence Act – AI Act* e, como já visto anteriormente, a proposta é que seja um documento sólido e flexível pelo qual discipline-se o tema da IA no âmbito de seus Países-Membros, bem como também tem o intuito de influenciar outros ordenamentos jurídicos para a elaboração de legislações semelhantes. O Parlamento Europeu atribuiu como prioridade o estabelecimento de normas alinhadas aos princípios e valores europeus para garantir que os sistemas de IA desenvolvidos e utilizados sob seu domínio legal sigam preceitos como a revisão humana, a transparência, a segurança, a privacidade, a não-discriminação e que também promovam o bem-estar social e ambiental[286].

O *AI Act* apresenta-se com o objetivo de ser um instrumento legal horizontal pelo qual será estabelecida uma abordagem baseada pelo nível de risco proporcionado pelos sistemas de IA, pelo que apresentam-se várias categorias de ameaças, como risco inaceitável, elevado, baixo ou mínimo. Sendo assim, há a estipulação de proibições e obrigações para cada grau, bem como de códigos de conduta para aqueles que não apresentam um risco classificado como elevado.

---

[284] Os quatro atributos mencionados foram indicados como princípios para o desenvolvimento de uma governança em IA por meio de um relatório apresentado com recomendações pelos auditores da KPMG. KPMG. **The shape of AI Governance to come**. KPMG International, 2021. Disponível em: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2021/01/the-shape-of-ai-governance-to-come.pdf> Acesso em set. 2023; LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 117.

[285] NEUWIRTH, Rostam J. **Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)**. Computer Law and Security Review, v. 48, p. 105798, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000092> Acesso em ago. 2023. p. 2.

[286] EUROPEAN PARLIAMENT. **Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM (2021) 0206 – C9 0146/2021 – 2021/0106 (COD))**. 2023. Disponível em: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf> Acesso em jun. 2023.

São, portanto, consideradas práticas de IA proibidas aquelas capazes de gerar um risco inaceitável por violarem os valores defendidos pela União Europeia, dos quais os direitos fundamentais fazem parte. Isso significa que os sistemas os quais apresentam um alto potencial de dano aos direitos das pessoas não podem ser admitidos, nem mesmo disponibilizados no mercado ou em serviço ou utilizados.

Nesta classificação, são compreendidos os sistemas de IA conhecidos como práticas subliminares, práticas de exploração, sistemas de pontuação social, bem como os sistemas de identificação biométrica remota em tempo real[287]. Cada um destes tipos impõe diferentes análises regulamentares, dadas as complexidades de suas naturezas, seus propósitos e suas consequências. No entanto, tendo em vista o escopo da presente investigação, apenas as primeiras serão mencionadas.

Nos termos do artigo 5º, parágrafo 1, alínea "a", no título II do regulamento proposto[288], entendem-se como práticas de IA proibidas os sistemas que, por meio de técnicas subliminares ou propositalmente manipuladoras ou enganosas, sejam capazes de distorcer a consciência das pessoas para obter como resultado a alteração de seus comportamentos, de modo que sejam provocados ou mesmo suscetíveis de ocasionar danos físicos ou psicológicos, tanto a quem com eles diretamente interage ou a outros indivíduos, bem como prejudicar sua capacidade de tomar uma decisão informada, a qual em outras circunstâncias não tomaria. Na alínea "b" do mesmo parágrafo, também são compreendidos como inaceitáveis os sistemas que explorem quaisquer vulnerabilidades de uma pessoa ou grupo de pessoas relacionadas a atributos como a faixa etária, as características de sua personalidade, a sua situação social e econômica ou a sua capacidade física ou mental, para que com isso seja possível empregar a distorção de suas consciências e a modificação de seus comportamentos, com o propósito de causar-lhe significativos danos físicos ou psicológicos[289].

---

[287] NEUWIRTH, Rostam J. **Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)**. Computer Law and Security Review, v. 48, p. 105798, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000092> Acesso em ago. 2023. p. 3.

[288] As demais especificidades descritas nas alíneas "c" e "d" do artigo 5º, parágrafo 1, não são consideradas como relevantes para os fins da presente investigação.

[289] O artigo 5º, parágrafo 1, alíneas "a" e "b" sofreram alterações em sua redação originalmente proposta, pelo que passaram, após emenda aprovada, a dispor da seguinte forma, *in verbis*: *"1. The following artificial intelligence practices shall be prohibited: (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a person or a specific group of persons, including characteristics of such person's or a such group's known or predicted personality traits or social or economic situation age, physical or mental ability with the objective or to the effect of materially distorting the behaviour of that person*

Isto posto, verifica-se que no *AI Act* não há uma proibição à utilização, à disponibilização no mercado ou a colocação em serviços de sistemas de IA que empreguem técnicas subliminares de uma forma geral, para outras finalidades. A vedação presente é imposta àqueles que tenham os objetivos especificados, ou seja, a distorção da consciência das pessoas e, em consequência, a alteração de seus comportamentos, bem como os efeitos previstos, isto é, que sejam suscetíveis de causar danos físicos ou psicológicos.

Embora na redação do regulamento proposto não seja claramente mencionado o termo *dark patterns* ou qualquer outro sinônimo pelo qual pudessem tais práticas serem indicadas, verifica-se que é possível compreender essas técnicas dentro da primeira alínea referida, pois conforme já mencionado, são constituídas por sistemas de IA os quais possuem essas mesmas características e têm a capacidade de causar os mesmos efeitos citados. Para além disso, caso seja feito um recorte sobre um público-alvo específico, como sobre a sua aplicação em relação a menores, idosos ou ainda pessoas com alguma deficiência, associando a determinadas práticas obscuras inseridas no contexto de um determinado tipo de modelo de negócio, como jogos *online*, compras virtuais ou mesmo as redes sociais, escopo da presente pesquisa, também podem ser visualizados tais padrões. Isso porque pessoas de grupos considerados vulneráveis podem ter uma menor capacidade de perceber e identificar tais técnicas, além de serem menos conscientes sobre seus efeitos e de que seu comportamento no ambiente digital pode estar sendo influenciado for fatores subliminares[290].

No entanto, critica-se a redação de tal artigo proposto em razão de apresentar uma conceituação percebida como vaga, visto que não menciona expressamente as definições legais dos termos utilizados[291]. Aponta-se uma ausência de clareza nos conceitos empregados, pois, por exemplo, embora no considerando número 16 até conste uma breve descrição do que pode

---

or a person pertaining to that group in a manner that causes or is likely to cause that person or another person significant harm; EUROPEAN PARLIAMENT. **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD))**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf> Acesso em set. 2023.

[290] EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them**. Version 2.0. February, p. 1–74, 2023. Disponível em: <https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> Acesso em set. 2023.

[291] BERMÚDEZ, Juan Pablo *et al*. **What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence**. 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS). West Lafayette, UNITED STATES OF AMERICA, 2023. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/document/10155039> Acesso em set. 2023; FRANKLIN, Matija; TOMEI, Philip; GORMAN, Rebecca. **Vague concepts in the EU Ai Act will not protect citizens from AI manipulation**. OECD.AI Policy Observatory, 2023. Disponível em: <https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions> Acesso em set. 2023.

ser entendido como técnicas subliminares[292], não parece ser o suficiente para esclarecer quais tipos de sistemas de IA estariam de fato englobados nessa proibição. Ainda, não há a menção clara ao que pode ser entendido, nos termos do referido documento legal, por traços de personalidade, pelo que são sugeridas alterações para traços psicológicos em vista de incrementar a efetividade da lei, uma vez que o termo empregado constitui apenas a uma parcela dos traços psicológicos das pessoas que podem ser atingidos por tais técnicas[293].

Não obstante, em que pese o artigo 5º, parágrafo 1, mencione de uma forma geral sistemas de IA que empreguem técnicas subliminares ou técnicas propositalmente manipuladoras ou enganosas, há recomendações para a separação de tais conceitos, visto que podem corresponder a métodos e objetivos diferentes[294]. Isso porque verifica-se que as técnicas subliminares têm o intuito de influenciar o comportamento de uma pessoa de modo que não seja possível de perceber tal ação. Já as técnicas manipuladoras seriam identificadas por meio de palavras-chave como o incentivo, a intenção, a dissimulação e o dano.

---

[292] O considerando número 16, após a aprovação da emenda número 38, passou atualmente a constar da seguinte forma, *in verbis*: *"(16) The placing on the market, putting into service or use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. This limitation should be understood to include neuro-technologies assisted by AI systems that are used to monitor, use, or influence neural data gathered through brain-computer interfaces insofar as they are materially distorting the behaviour of a natural person in a manner that causes or is likely to cause that person or another person significant harm. Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of individuals and specific groups of persons due to their known or predicted personality traits, age, physical or mental incapacities, social or economic situation. They do so with the intention to or the effect of materially distorting the behaviour of a person and in a manner that causes or is likely to cause significant harm to that or another person or groups of persons, including harms that may be accumulated over time. The intention to distort the behaviour may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user, such as factors that may not be reasonably foreseen and mitigated by the provider or the deployer of the AI system. In any case, it is not necessary for the provider or the deployer to have the intention to cause the significant harm, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices is complementary to the provisions contained in Directive 2005/29/EC, according to which unfair commercial practices are prohibited, irrespective of whether they carried out having recourse to AI systems or otherwise. In such setting, lawful commercial practices, for example in the field of advertising, that are in compliance with Union law should not in themselves be regarded as violating prohibition. Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in humanmachine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research and on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian."* EUROPEAN PARLIAMENT. **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD))**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf> Acesso em set. 2023.

[293] FRANKLIN, Matija; TOMEI, Philip; GORMAN, Rebecca. **Vague concepts in the EU Ai Act will not protect citizens from AI manipulation**. OECD.AI Policy Observatory, 2023. Disponível em: <https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions> Acesso em set. 2023.

[294] FRANKLIN, Matija; TOMEI, Philip; GORMAN, Rebecca. **Vague concepts in the EU Ai Act will not protect citizens from AI manipulation**. OECD.AI Policy Observatory, 2023. Disponível em: <https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions> Acesso em set. 2023.

Desta forma, pelo incentivo, os sistemas recebem certos incentivos em seu treinamento para influenciar intencionalmente o comportamento das pessoas; já pela intenção, tais métodos são usados propositalmente para atingir uma meta determinada, fazendo parte essencial do processo de como a mudança de comportamento dos indivíduos pode resultar em um dado objetivo. Por sua vez, há a dissimulação, pela qual a pessoa, sobre a qual tais técnicas estão sendo utilizadas, não é capaz de compreender significativamente o que o sistema de IA está realizando sobre si, nem mesmo os impactos dessas ações. Pelo dano, por fim, as ações de um sistema são capazes de afetar negativamente as pessoas e causar repercussões sobre seus comportamentos. Além disso, as técnicas enganosas seriam aquelas pelas quais um sistema de IA apresenta-se fingindo ter uma finalidade, mas possui outra, oculta, pela qual é operado. Assim, distorce materialmente a compreensão sobre si, ao criar impressões falsas sobre seu funcionamento, objetivos e efeitos. Em vista disso, pode alterar a consciência e o comportamento das pessoas e influenciar suas preferências, manipulando ou ocultando as opções, as informações importantes ou até exibindo-as de forma incompleta, bem como seus resultados[295].

Por isso, para uma maior efetividade da lei, é importante que não haja lacunas para possibilitar interpretações e aplicações enviesadas, de modo que recomenda-se o esclarecimento dos termos utilizados na confecção das proibições. Isso porque uma definição clara traduz-se em transparência e compreensão do regulamento legal, o que não somente pode fortalecer as normas e enfatizar a proteção dos direitos fundamentais envolvidos, como também estimular o desenvolvimento tecnológico de forma responsável e ética. Uma estrutura regulatória fortemente estrita poderia influenciar negativamente o desenvolvimento da área da IA, restringindo-o, mas uma legislação branda e com espaço para interpretações diversas poderia, para além de representar uma regulação insuficiente e meramente simbólica, gerar insegurança jurídica.

Já no que tange ao regime de sanções previstas, nos termos do artigo 71º, parágrafo 1, estabelece-se que, em caso de infração às normas reguladoras da IA no âmbito da União Europeia, seus Estados-Membros devem dispor dos mecanismos necessários para a aplicação da lei[296]. Assim, segundo o parágrafo 3 do mesmo artigo, quando houver o descumprimento

---

[295] CARROLL, Micah *et al*. **Characterizing Manipulation from AI Systems**. Association for Computing Machinery, 2023. v. 1. Disponível em: <https://arxiv.org/pdf/2303.09387.pdf> Acesso em set. 2023.

[296] O artigo 71º, parágrafo 1, do texto proposto e emendado, *in verbis*: *"Article 71. Penalties. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, applicable to infringements of this Regulation by any operator, and shall take all measures necessary to ensure that they are properly and effectively implemented and aligned with the guidelines issued by the Commission and the AI Office pursuant to Article 82b. The penalties provided for shall be effective, proportionate, and dissuasive.*

das práticas de IA proibidas no mencionado artigo 5º, como penalidade pode ser arbitrada uma multa de até 40.000.000 € (quarenta milhões de euros) ao infrator. Na hipótese de o descumpridor ser uma empresa, tal punição pode corresponder a até 7 % (sete por cento) de seu volume de negócios anual a nível mundial no exercício anterior, de acordo com o que corresponder a um valor mais elevado[297].

Desta forma, observa-se que a União Europeia tem reconhecido que essas técnicas em sistemas de IA têm a alta capacidade de produzir danos prejudiciais às pessoas, sendo entendidas como práticas abusivas e que, em razão disso, devem ser proibidas. Isso porque, como visto, não correspondem aos valores do Estado Democrático de Direito apoiados pelos países do bloco, sobretudo as liberdades, a igualdade, a privacidade e os direitos das crianças e adolescentes, bem como outros direitos já previstos em outras legislações como a proteção de dados pessoais, não-discriminação e leis de direito dos consumidores e de concorrência[298]. Por fim, sobre o estado da tramitação legislativa do referido documento de regulação, até o presente momento foi adotada a posição de negociação da proposta do *AI Act* pelos eurodeputados, para que então passe à fase de tratativas com os Países-Membros no Conselho a respeito de seu formato final[299].

Por sua vez, o Brasil também possui uma proposta de regulação da IA em andamento atualmente, qual seja, o Projeto de Lei n. 21/2020. Por ter um processo legislativo de forma bicameral, o referido documento legal recebeu aprovação quando apresentado à Câmara dos

---

They shall take into account the interests of SMEs and start-ups and their economic viability." EUROPEAN PARLIAMENT. **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD))**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf> Acesso em set. 2023.

[297] O artigo 71º, parágrafo 3, de acordo com o novo texto proposto por emenda e aprovado, in verbis: *"3. Non compliance with the prohibition of the artificial intelligence practices referred to in Article 5 shall be subject to administrative fines of up to 40 000 000 EUR or, if the offender is a company, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher."* EUROPEAN PARLIAMENT. **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD))**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf> Acesso em set. 2023.

[298] EUROPEAN PARLIAMENT. **Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM (2021) 0206 – C9 0146/2021 – 2021/0106 (COD))**. 2023. Disponível em: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf> Acesso em set. 2023. p. 126.

[299] EUROPEAN PARLIAMENT. **MEPs ready to negotiate first-ever rules for safe and transparent AI**. News, 14 jun. 2023. Disponível em: <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai> Acesso em set. 2023.

Deputados, mas sofreu diversas alterações quando foi enviado ao Senado Federal. Por conta disso, conforme já visto, foi elaborado um novo texto, substitutivo ao anterior e apresentado no fim do ano de 2022.

A proposta brasileira de regulação da IA apresenta-se com duas finalidades, sendo por um lado assegurar direitos para a proteção das pessoas que de alguma forma são impactadas pelos sistemas de IA e, por outro, oferecer mecanismos de governança e uma estrutura institucional para a fiscalização e supervisão de tais tecnologias, de modo a fornecer parâmetros e segurança jurídica para a inovação e o desenvolvimento econômico, tecnológico e científico. Seguindo uma perspectiva semelhante ao projeto europeu, busca estabelecer também uma abordagem com base nos riscos produzidos por esses sistemas, sendo um modelo regulatório firmado na proteção dos direitos fundamentais, uma vez que tem como núcleo a dignidade da pessoa humana. Como fundamentos para o desenvolvimento, implementação e uso da IA em seu território, propõe uma harmonização entre valores como a proteção dos direitos e liberdades fundamentais e a valorização do trabalho e os princípios da ordem econômica, com o estímulo à formação de novas cadeias de valor[300].

Em seu texto, a proposta traz proibições e obrigações diferentes quanto ao risco oferecido pelos sistemas de IA, os quais deverão passar por uma avaliação preliminar por seu fornecedor, previamente à sua disponibilização no mercado ou utilização de seu serviço, para a sua devida classificação e registro. Sendo assim, em sua seção II, dedicada àqueles entendidos como de risco excessivo, dispõe em seu artigo 14, inciso I que são vedadas a implementação e o uso de IA que utilize técnicas subliminares com a intenção de alterar o comportamento da pessoa natural, representando prejuízos ou perigos à sua saúde ou segurança, bem como que sejam incompatíveis com os direitos reconhecidos como fundamentos da proposta. Além disso, prevê em seu inciso II a vedação aos sistemas que pratiquem a exploração das vulnerabilidades de grupos de pessoas naturais, isto é, em razão de sua idade ou deficiência física ou mental, para assim provocar a distorção de seus comportamentos, nos mesmos moldes de como previsto no inciso anterior[301].

---

[300] SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em set. 2023. p. 9-10.

[301] Nos termos da redação do artigo 14, caput e incisos I e II, *in verbis*: "Art. 14. São vedadas a implementação e uso de sistemas de inteligência artificial: I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos deste lei; II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como associadas à sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma

Ademais, estabelece em seu artigo 16 que caberá à autoridade competente a regulamentação dos sistemas considerados de risco excessivo, o que demonstra que pode haver a futura possibilidade de admissão de alguma determinada técnica, ainda que não mencionadas em quais condições nem para quais finalidades. Embora não designada na proposta, prevê apenas que essa autoridade será um órgão ou entidade da Administração Pública Federal, cuja competência será o zelo, a implementação e a fiscalização do cumprimento das normas regulatórias em todo o território brasileiro[302].

Por sua vez, na seção II sobre as sanções administrativas, a proposta estabelece ainda, em seu artigo 36, que os agentes de IA estarão sujeitos, em razão das infrações às normas do regulamento e sua gravidade, tais como as violações de direitos, a penalidades como a advertência e multa simples limitada no total de R$ 50.000.000,00 (cinquenta milhões de reais) por cada descumprimento. Sendo o infrator pessoa jurídica de direito privado, tal punição pode chegar a até 2 % (dois por cento) do volume de negócios no último exercício financeiro do grupo ou conglomerado de suas empresas no Brasil, sendo excluídos os tributos. Além disso, constam no rol de sanções outras medidas como a publicidade da infração, a proibição ou restrição pelo prazo de até cinco anos para participação de regimes regulatórios de *sandbox*[303], ou até mesmo a suspensão parcial ou total, temporária ou definitiva das atividades de desenvolvimento, fornecimento ou operação de sistemas de IA[304].

---

prejudicial à sua saúde ou segurança ou contra os fundamentos desta lei;" SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em set. 2023. p. 28.

[302] Transcrição do artigo 16 da proposta regulatória brasileira: "Art. 16. Caberá à autoridade competente regulamentar os sistemas de inteligência artificial de risco excessivo." SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em set. 2023. p. 29.

[303] Entende-se por *sandbox* um ambiente virtual independente e isolado para testar e executar programas, códigos e *sotfwares* em desenvolvimento, sem afetar o sistema ou a rede, evitando assim que possíveis falhas e vulnerabilidades causem algum impacto.

[304] O artigo 36 proposto, em destaque dos trechos mencionados: "Art. 36. Os agentes de IA, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade competente: I – advertência; II – multa simples, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, sendo, no caso de pessoa jurídica de direito privado, de até 2% (dois por cento) de seu faturamento, de seu grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos; III – publicização da infração após devidamente apurada e confirmada a sua ocorrência; V – proibição ou restrição para participar de regime de sandbox regulatório previsto nesta lei, por até cinco anos; e IV – suspensão parcial ou total, temporária ou definitiva, do desenvolvimento, fornecimento ou operação do sistema de inteligência artificial; VI – proibição de tratamento de determinadas bases de dados. § 1º As sanções serão aplicadas após procedimento

Apesar de que, mais uma vez, a questão dos *dark patterns* não foi expressamente mencionada, nem mesmo por outro termo semelhante, é possível depreender que, nas alíneas destacadas do artigo 14, pode-se encontrar a proibição a tais técnicas manipuladoras, tendo em vista que os sistemas tratados apresentam semelhantes propriedades, bem como podem ter um similar potencial de controle sobre o comportamento das pessoas. Além disso, também entende-se a sua proibição no tocante à sua aplicação para determinados segmentos de pessoas, como por fatores como a idade ou a deficiência física e mental.

Assim como ocorrido com a proposta de regulação europeia nos artigos destacados sobre as práticas proibidas, verifica-se que também não houve uma clara definição legal de conceitos importantes para o estabelecimento das vedações aos sistemas considerados de risco excessivo. Isso porque não foi explicado, na perspectiva da lei proposta, o que seriam as técnicas subliminares, nem mesmo o que seria entendido como forma prejudicial ou perigosa à sua saúde ou segurança, o que pode acarretar questões semelhantes às indicadas no tocante ao espectro europeu. Já sobre a última parte do inciso I do artigo 14, isto é, acerca dos fundamentos da lei, houve a indicação de que tais fundamentos estão elencados no rol presente nos dez incisos do artigo 2º, como por exemplo o livre desenvolvimento da personalidade, o respeito aos direitos humanos e aos valores democráticos, a privacidade, a proteção de dados e o acesso à informação[305].

---

administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I – a gravidade e a natureza das infrações e a eventual violação de direitos; II – a boa-fé do infrator; III – a vantagem auferida ou pretendida pelo infrator; IV – a condição econômica do infrator; V – a reincidência; VI – o grau do dano; VII – a cooperação do infrator; VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar riscos, inclusive a análise de impacto algorítmico e efetiva implementação de código de ética; IX – a adoção de política de boas práticas e governança; X – a pronta adoção de medidas corretivas; XI – a proporcionalidade entre a gravidade da falta e a intensidade da sanção; XII – a cumulação com outras sanções administrativas eventualmente já aplicadas em definitivo para o mesmo ato ilícito. [...] **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em set. 2023. p. 51-54.

[305] De acordo com o artigo 2º proposto, *in verbis*: "Art. 2º O desenvolvimento, implementação e uso de sistemas de inteligência artificial no Brasil têm como fundamentos: I – a centralidade da pessoa humana; II – o respeito aos direitos humanos e aos valores democráticos; III – o livre desenvolvimento da personalidade; IV – a proteção ao meio ambiente e o desenvolvimento sustentável; V – a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas; VI – o desenvolvimento tecnológico e a inovação; VII – a livre iniciativa, a livre concorrência e a defesa do consumidor; VIII – a privacidade, a proteção de dados e a autodeterminação informativa; IX – a promoção da pesquisa e do desenvolvimento com a finalidade de estimular a inovação nos setores produtivos e no poder público; X – o acesso à informação e à educação, bem como a conscientização sobre os sistemas de inteligência artificial e suas aplicações." **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a**

Desta forma, observa-se uma espécie de alinhamento entre os projetos de regulação da IA europeu e brasileiro, pelo que seguem um mesmo sentido de equilíbrio entre a proteção garantida aos direitos fundamentais, já assegurados em outros documentos legais, e o estímulo ao desenvolvimento tecnológico, à livre iniciativa, à livre concorrência e à inovação. Considerando que muitas empresas desenvolvedoras e detentoras de sistemas de IA são multinacionais instaladas e com atividade em diversas partes do mundo, percebe-se como positivo esse ajuste entre legislações de países distintos, a fim de proporcionar um entendimento em harmonia e concordância sobre a proteção dos direitos fundamentais em diferentes ordenamentos jurídicos. No entanto, assim como visto na proposta europeia, há também lacunas no esclarecimento de termos e expressões empregadas no texto da lei que precisam de serem elucidadas, a fim de garantir a máxima efetividade à lei futura e aos seus dispositivos, não deixando margem para interpretações que de alguma forma exponham os direitos envolvidos a algum risco ou violação.

Sobre o estado atual de sua tramitação, como última movimentação registrada foi determinado que o Projeto de Lei n. 21/2020 passará a tramitar em conjunto com outras propostas, os quais tratam de matérias semelhantes. Além disso, seguirão ao exame da Comissão Temporária sobre Inteligência Artificial no Brasil, designada para que o colegiado de senadores, por meio da realização de audiências públicas, possa discutir, com a participação da sociedade civil, o anteprojeto apresentado pela comissão de juristas[306].

Já no âmbito dos Estados Unidos da América, com o objetivo de proteger a inovação tecnológica e suas indústrias, visto que as principais empresas do ramo da tecnologia tem sede em seu território, verifica-se uma abordagem mais flexível e até mesmo considerada liberal para a regulação da IA. Isso porque entende-se que um documento legislativo mais moderado estimularia o desenvolvimento interno, aumentando com isso a competitividade do país a nível internacional. Ainda assim, para os estadunidenses é considerada fundamental a proteção dos direitos civis de seus cidadãos[307].

Desta forma, no tocante a uma regulação para a IA em âmbito estadunidense, no ano de 2019 foi apresentado pelo Governo Federal Estadunidense a Ordem Executiva número 13.859, um documento chamado *Maintaining American Leadership in Artificial Intelligence*,

---

aplicação da inteligência artificial no Brasil. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em set. 2023. p. 16.

[306] SENADO FEDERAL. **Despacho da Presidência do Senado Federal**. Diário do Senado Federal n. 140, pág. 93. Publicado em 17 de agosto de 2023. Brasília, 2023. Disponível em: <https://legis.senado.leg.br/diarios/ver/113434?sequencia=93> Acesso em set. 2023. p. 93.

[307] LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022. p. 126.

pelo qual foram estabelecidos princípios e políticas com a finalidade de fortalecer a liderança global científica, econômica e tecnológica do país no desenvolvimento da área da IA. Dentre os objetivos designados, estão o desenvolvimento de normas técnicas adequadas para promover a confiança nessas tecnologias, além de proteger a privacidade, as liberdades civis e os valores sustentados por seus cidadãos. Ademais, como princípios são elencados a cooperação internacional para uma IA confiável, a transparência e a explicabilidade, o crescimento inclusivo, a robustez e a segurança, bem como os valores centrados no ser humano e na justiça. Conhecido como *American AI Iniciative*, o referido documento foi proposto como uma política de governo na qual a regulação da IA constitui um de seus objetivos[308].

Posteriormente, dando seguimento às determinações da mencionada ordem executiva, no ano de 2021, por meio de seu *Office of Science and Technology Policy*, foi apresentado o documento *National Artificial Intelligence Initiative Office - NAIIO*, pelo qual foram indicados os princípios que as agências reguladoras federais devem observar para estabelecer as normas regulamentares para a IA em cada um dos seus setores específicos, como a flexibilidade, a participação do público, a coordenação interinstitucional e a confiança pública na IA[309]. Além disso, por tais princípios, foram limitados os alcances regulatórios de cada agência, para que, nessa abordagem setorial, seja construída uma estrutura de regulação com maior especificidade, evitando assim a designação de normas muito amplas, o que poderia levar a prejuízos em sua efetividade.

Recentemente, no presente ano de 2023, foi apresentado um projeto de lei com o objetivo de estabelecer uma estrutura organizacional para a governança e supervisão da IA para os Estados Unidos. Intitulado como *Assuring Safe, Secure, and Ethical Systems for AI Act* ou simplesmente *ASSESS AI Act*, a proposta consiste em designar a constituição de uma força tarefa para identificar lacunas nas políticas e legislações do governo federal estadunidense para a IA, bem como fornecer recomendações específicas de acordo com as necessidades apuradas. Sobre o estado atual de tramitação do referido texto, apenas foi apresentado e lido aos senadores, pelo que foi enviado ao *Committee on Commerce, Science, and Transportation*, não

---

[308] THE WHITE HOUSE. **Maintaining American Leadership in Artificial Intelligence**. Executive Order n. 13.859, of February 11, 2019. Disponível em: <https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf> Acesso em set. 2023.

[309] THE WHITE HOUSE. **National Artificial Intelligence Initiative Office (NAIIO)**. Division E, Title LI, Section 5102, 2021. Disponível em: <https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1213> Acesso em set. 2023.

tendo sido indicada data para discussão e votação até o presente momento, ou mesmo qualquer outra determinação[310].

Assim, não se verificou até então a existência de uma lei de regulação da IA a nível federal nos Estados Unidos da América, isto é, uma legislação horizontal que pudesse regular esta temática de uma forma geral. Pelo contrário, diferente das regulações propostas no âmbito da União Europeia e do Brasil, percebe-se a primazia por uma abordagem mais voltada à atuação setorial, de modo a respeitar as peculiaridades e necessidades que diferentes áreas, como a saúde, a educação, o consumo e os transportes, podem apresentar.

Sendo assim, no tocante a uma legislação específica que por algum meio trate a problemática dos *dark patterns* em âmbito estadunidense, pode ser referenciado um projeto de lei apresentado no ano de 2021, chamado *Deceptive Experiences to Online Users Reduction Act*, ou apenas *DETOUR Act*. Sobre o seu estado de tramitação, foi apenas anunciado aos senadores e encaminhado ao *Subcommittee on Consumer Protection and Commerce*, não tendo até o momento qualquer outra movimentação ou atividade. Busca-se com tal projeto estabelecer uma vedação ao uso de práticas exploradoras e enganosas por grandes operadores de serviços online, além da promoção do bem-estar dos consumidores. Tais operadores são entendidos, nos termos da lei, como qualquer pessoa que forneça um serviço online, que tenha mais de 100.000.000 (cem milhões) de usuários autenticados em um período de trinta dias e que estejam sujeitos à jurisdição da *Federal Trade Commission – FTC* e das normas dispostas na *Federal Trade Commission Act*, legislação em vigor desde o ano de 1914.

Pelo documento proposto, de acordo com a sua seção 3 (a) (1) (A), é entendido como conduta proibida e ilegal projetar, modificar ou manipular o *design* da interface de usuário com o propósito de prejudicar a autonomia dos utilizadores, sua tomada de decisão e a arquitetura de escolhas para obter seu consentimento e seus dados[311]. Ademais, ainda na mesma seção 3 (a) (1) (C), fica proibido o desenho, a modificação ou a manipulação da interface de usuário de um serviço *online* que tenha como público os menores de 13 (treze) anos, com o objetivo de

---

[310] O projeto de lei identificado como *ASSESS AI Act* foi apresentado pelo senador democrata Michael Bennet em abril de 2023. SENATE OF THE UNITED STATES OF AMERICA. **S. 1356**, **Assuring Safe, Secure, and Ethical Systems for AI Act,** 2023. Disponível em: <https://www.congress.gov/bill/118th-congress/senate-bill/1356/text> Acesso em set. 2023.

[311] A seção 3 (a) (1) (A), *in verbis*: *"SEC. 3. UNFAIR AND DECEPTIVE ACTS AND PRACTICES RELATING TO THE MANIPULATION OF USER INTERFACES. (a) CONDUCT PROHIBITED. — (1) IN GENERAL.—It shall be unlawful for any large online operator— (A) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data."* SENATE OF THE UNITED STATES OF AMERICA. **S. 1084, Deceptive Experiences to Online Users Reduction Act**, 2021. Disponível em: <https://www.congress.gov/116/bills/s1084/BILLS-116s1084is.pdf> Acesso em set. 2023.

causar o seu uso compulsivo, por meio do emprego de funções como o *dark pattern* de *autoplay* para a reprodução automática de arquivos de mídia de vídeo sem o consentimento do usuário[312].

Para a aplicação da referida legislação proposta, foi designada como a autoridade competente a *FTC*, visto que é a agência reguladora federal responsável pela proteção dos consumidores e pela promoção de um mercado competitivo, bem como que um descumprimento ao determinado na seção supramencionada seria tratada como violação das regras previstas pela *Federal Trade Commission Act*, no que tange às condutas injustas ou práticas enganosas. Assim, conforme já mencionado anteriormente, por esta lei, pode ser imposta uma penalidade civil de não mais que US$ 10.000,00 (dez mil dólares) por cada violação verificada. No caso de uma inobservância que incorra em propagandas enganosas com o objetivo de fraudar ou enganar o consumidor, será punido com o pagamento de multa não superior a US$ 5.000,00 (cinco mil dólares) ou prisão não superior a seis meses, ou ainda, as duas penalidades juntas[313].

Por tudo isso, observa-se que nos diferentes ordenamentos jurídicos analisados há abordagens distintas não somente para a regulação da inteligência artificial como um todo, como também para o enfrentamento do problema causado pelos *dark patterns*. Verificou-se uma consonância entre as propostas europeia e brasileira, tanto na formulação dos dispositivos que podem tratar a questão de tais padrões obscuros, como nas lacunas sobre os termos empregados no texto que ainda carecem de esclarecimento. Já no caso dos EUA, percebeu-se a preferência por uma abordagem setorial, de modo qu

Por meio da tutela dos direitos fundamentais, a exemplo da proteção de dados pessoais, ou invocando os direitos do consumidor, têm-se buscado combater de alguma forma tais padrões obscuros. No entanto, percebe-se a dificuldade que os legisladores têm encontrado em definir os conceitos e terminologias relacionadas ao tema para eliminar possíveis lacunas e garantir a máxima efetividade ao texto legal. Considerando que a tecnologia é uma ciência em constante transformação, vê-se o dilema dos países em estabelecer um equilíbrio entre delinear parâmetros normativos estritos mas ainda incentivar a inovação, ou propor regras mais flexíveis e tornar a legislação pouco eficaz aos seus fins.

---

[312] A seção 3 (a) (1) (C), *in verbis*: *"(C) to design, modify, or manipulate a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of, with the purpose or substantial effect of cultivating compulsive usage, including video auto-play functions initiated without the consent of a user."* SENATE OF THE UNITED STATES OF AMERICA. **S. 1084, Deceptive Experiences to Online Users Reduction Act**, 2021. Disponível em: <https://www.congress.gov/116/bills/s1084/BILLS-116s1084is.pdf> Acesso em set. 2023.

[313] FEDERAL TRADE COMMISSION. **Federal Trade Commission Act incorporating U.S. SAFE WEB Act Amendments of 2006**. Disponível em: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim> Acesso em jun. 2023.

6 CONCLUSÃO

A presente pesquisa buscou investigar o problema decorrente da aplicação dos *dark patterns* no *design* das interfaces de usuário das redes sociais, com o objetivo de distorcer a consciência das pessoas e, consequentemente, alterar seus comportamentos. Isso porque tais empresas utilizam-se de mecanismos de IA para manipular a atividade na plataforma e influenciar as decisões de seus usuários, na medida em que exercem um poder de controle sobre a oferta de opções, a apresentação e o encontro de informações importantes e a exibição de publicações e publicidades. Com isso, ocorrem violações a diversos direitos fundamentais dos usuários, como a privacidade, a proteção de dados pessoais, a autodeterminação informativa, as liberdades de consciência, expressão, comunicação e de informação, os direitos difusos e coletivos como os direitos do consumidor e, em último grau, a dignidade da pessoa humana.

Após a análise de tal problemática, questionou-se a existência de medidas legais satisfatórias nos ordenamentos jurídicos destacados para fornecer a necessária proteção aos direitos fundamentais atingidos. Em outras palavras, diante dessas novas formas de violações e riscos a direitos, indagou-se quais dispositivos legais já existentes podem ser aplicados para promover a defesa dos bens jurídicos envolvidos, bem como se as propostas legislativas que buscam desenvolver um documento regulatório para a inteligência artificial seriam alternativas suficientemente eficazes ou, ainda, se haveria a necessidade de apresentar um novo dispositivo legal para servir a essa função.

Desta forma, observou-se que não se dispõe até o momento de uma medida jurídica especialmente elaborada com o objetivo de enfrentar e proibir tais práticas em sua totalidade, havendo, portanto, uma lacuna legislativa sobre o tema. Por outro lado, verificou-se que há a existência de documentos legais acerca de temáticas como a proteção de dados pessoais, tendo em vista que a essência do funcionamento desse tipo de empresas é a coleta de dados pessoais de seus usuários, bem como que muitos padrões desvirtuam o consentimento fornecido sobre o acesso a tais informações, além das leis de proteção dos direitos do consumidor, uma vez que a relação estabelecida entre o usuário, consumidor do serviço e a plataforma de rede social, fornecedora, pode ser entendida como de consumo.

Desta forma, na União Europeia há leis do campo digital que podem ter alguma aplicação para a questão dos *dark patterns*, a exemplo do *DSA* e do *DMA*. No entanto, considerando que essas legislações são recentes, ainda não é possível averiguar sua efetividade no que tange à resolução do problema em questão. Além disso, podem ser aplicadas as normas de proteção de dados pessoais constantes no *GDPR*, porém verificou-se que não fornecem

cobertura a todos os tipos de padrões, já que nem todos têm uma ligação direta com os dados pessoais. Assim como no referido bloco, no Brasil foram percebidas as mesmas questões, isto é, apurou-se que há a possibilidade de aplicação das normas de proteção de dados pessoais e das leis de proteção ao direito do consumidor, uma vez que não há lei específica para tratar os *dark patterns*. Entretanto, visualizam-se os mesmos obstáculos no que tange à sua efetividade, já que os dispositivos da LGPD não têm incidência sobre todas as espécies de técnicas, bem como que demandaria um exercício de interpretação exaustiva para aplicar as normas constantes no CDC para a situação.

Ainda, tendo em vista a primazia por uma abordagem setorial nos EUA e a autonomia de seus estados federados para debater temas desse tipo, foram destacadas algumas legislações estaduais que, ao versarem sobre questões como a privacidade e os direitos do consumidor, de alguma forma trataram o tópico. Dada a escassez normativa aferida nos sistemas legais analisados, concluiu-se que há a necessidade de um texto normativo que aborde diretamente a situação dos *dark patterns* inseridos no *design* do ambiente digital de *sites*, aplicativos e plataformas, de modo a abranger todos os seus mais variados tipos, para que seja então oferecida a proteção devida aos direitos fundamentais que estão vulneráveis a esses padrões obscuros e seus efeitos.

Para regular o desenvolvimento, a implementação e a utilização de sistemas de inteligência artificial de um modo geral e por esse meio tratar o mencionado assunto, há algumas propostas apresentadas na União Europeia, no Brasil e nos Estados Unidos da América. No entanto, embora não façam referência expressa ao termo nem a qualquer outro sinônimo, ao mencionar em outras palavras os sistemas de IA com as mesmas características, efeitos e finalidades, entende-se que estão a abordar o referido tópico. Para além disso, percebeu-se a necessidade de esclarecer alguns termos e expressões utilizados em tais propostas legislativas, a fim de garantir a efetividade esperada dessas futuras leis.

Ao final, verificou-se também que, como a situação dos *dark patterns* nas redes sociais constitui um conflito entre direitos fundamentais, pode-se recorrer à via da interpretação constitucional para realizar uma harmonização dos direitos envolvidos e seus âmbitos de proteção, a fim de viabilizar uma solução ao problema. Assim, atualizar-se-ia o texto constitucional para, por meio da interpretação da norma, oferecer uma resolução adaptada à situação e suas peculiaridades.

Em vista de tais considerações, acredita-se que a presente pesquisa contribuiu para ampliar não somente o debate acerca da regulação da IA, mas sobre os *dark patterns* de uma forma geral, sejam eles inseridos nas redes sociais ou em qualquer ambiente digital, visto que

oferecem riscos significativos aos direitos que com eles de algum modo são envolvidos. Observa-se que a temática é recente e ainda demanda o amadurecimento das discussões a fim de construir as soluções adequadas à situação e os seus problemas decorrentes.

Considerando que a inteligência artificial é uma ciência concebida com a característica da transdisciplinaridade, deve-se também reconhecer que a questão de tais padrões obscuros necessita de um debate plural. Ao englobar as várias áreas envolvidas e suas diferentes perspectivas, como o *design*, a própria IA, o direito e a ética, entre outros, podem ser pensadas e desenvolvidas alternativas para um *design* ético e equilibrado entre os interesses de negócio das empresas e as necessidades e direitos dos usuários.

Para além disso, tal debate deve também envolver a sociedade como um todo, visto que muitas pessoas são usuárias de redes sociais e utilizam-nas para diversas funcionalidades diariamente, sem ter conhecimento, contudo, de que sua atividade na plataforma, bem como seus comportamentos dentro e até mesmo fora dela, estão sendo afetados e manipulados por essas interferências obscuras. A informação deve ser uma importante ferramenta para que inclusive os próprios usuários possam cobrar medidas e mudanças às plataformas e aos legisladores, para que sejam desenvolvidos sistemas de IA com princípios éticos e que respeitem os direitos fundamentais das pessoas. Ou, pelo menos, que a informação sirva de alerta para que os usuários saibam como reagir e de alguma forma protegerem-se contra essas práticas abusivas.

Neste sentido, compreende-se que as investigações futuras podem abordar a questão dos *dark patterns* inseridos em outros tipos de *sites*, aplicativos e plataformas e suas mais variadas espécies, tendo em vista que alguns são essencialmente elaborados para finalidades determinadas. Além disso, pode-se pesquisar os impactos e problemas decorrentes de sua aplicação voltada para um público-alvo específico, como para menores de idade, idosos ou pessoas com pouca alfabetização tecnológica, os quais podem ser considerados como mais vulneráveis e suscetíveis aos efeitos e danos.

Com o avanço do desenvolvimento, da implementação e da utilização de sistemas de IA, percebe-se que a vida humana têm sido permeada pela aplicação de ferramentas de tecnologia e por decisões automatizadas em muitas áreas e para várias finalidades. Por onde a inteligência artificial atravessa, carrega transformações e impõe mudanças. Ao lado de diversos benefícios, há de se constatar também as novas modalidades de violações e riscos a direitos fundamentais, pelo que tais mudanças devem ser acompanhadas por respostas congruentes para garantir a máxima tutela aos bens jurídicos em evidência. Desta forma, regular a IA é providência que mostra-se como necessária, tanto para abalizar a inovação e o desenvolvimento

científico, quanto para assegurar a devida proteção aos direitos fundamentais, visto que os sistemas legais, para alguns casos, podem carecer de medidas eficazes para resolver as questões decorrentes de seu uso.

Em uma visão “kantiana” da dignidade da pessoa humana, entende-se que as pessoas devem ser tratadas como um fim em si mesmas, e não como apenas um meio, isto é, meros objetos pelos quais atinge-se um determinado objetivo. Os fins não podem justificar os meios e, neste caso, as redes sociais não podem utilizar-se da tecnologia dos sistemas de IA e de meios ardilosos para exercer um poder de controle sobre seus usuários, influenciando negativamente suas escolhas e seus comportamentos para que atendam aos seus escusos interesses de negócio e, de qualquer forma, obterem lucro. Pelo contrário, devem as redes sociais servirem como novos instrumentos para que as pessoas possam manifestar e exercer seus direitos e liberdades, promovendo assim a justa proteção desses direitos, fundamentais até mesmo no ambiente digital.

REFERÊNCIAS

AHUJA, Sanju; KUMAR, Jyoti. **Conceptualizations of user autonomy within the normative evaluation of dark patterns**. Ethics and Information Technology, v. 24, n. 4, p. 1–18, 2022. Disponível em: <https://doi.org/10.1007/s10676-022-09672-9> Acesso em jun. 2023.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. de Virgílio Afonso da Silva. – 2. ed. São Paulo: Malheiros Editores, 2015.

ASIMOV, Isaac. **Eu, robô**. Trad. Aline Storto Pereira. - São Paulo: Aleph, 2015. Disponível em: <https://ia801503.us.archive.org/17/items/Livros-isaac-asimov/Eu%2C_Robo_-_Isaac_Asimov.pdf> Acesso em nov. 2022.

BARBOSA, Mafalda Miranda. **Inteligência Artificial: entre a utopia e a distopia, alguns problemas jurídicos**. 1. ed. Coimbra: Gestlegal, 2021.

BARONI, Luiz Adolpho *et al*. **Dark Patterns: Towards a Socio-technical Approach**. ACM International Conference Proceeding Series, 2021. Disponível em: <https://dl.acm.org/doi/abs/10.1145/3472301.3484336> Acesso em jul. 2023.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: Os Conceitos Fundamentais e a Construção do Novo Modelo**. – 2. ed. São Paulo: Saraiva, 2010.

BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. **AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience**. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 48, n. October 2021, p. 105767, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922001108?via%3Dihub> Acesso em jan. 2023.

BELLI, Luca; ZINGALES, Nicolo. **Data protection and artificial intelligence inequalities and regulations in Latin America**. Computer Law & Security Review, v. 47, p. 105761, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922001042> Acesso em jan. 2023.

BERMÚDEZ, Juan Pablo *et al*. **What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence**. 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS). West Lafayette, USA, 2023. p. 1–10. Disponível em: <https://ieeexplore.ieee.org/document/10155039> Acesso em set. 2023.

BIETTI, Elettra. **A Genealogy of Digital Platform Regulation**. Georgetown Law Technology Review, 1, 2023. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859487> Acesso em ago. 2023. p. 30.

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de janeiro: Forense, 2019.

BODEN, Margareth A. **AI: its nature and future**. Oxford: Oxford University Press, 2016.

BODEN, Margareth A. **Mind as machine: a history of cognitive science**. v. 1. Oxford: Oxford University Press, 2006.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. – 15. ed. São Paulo: Malheiros Editores, 2004.

BRASIL. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Brasília: MCTIC, 2021. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf> Acesso em fev. 2023.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobe a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor – CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm> Acesso em set. 2023.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em set. 2023.

BRIGNULL, Harry. **Dark Patterns: inside the interfaces designed to trick you**. The Verge, 2013. Disponível em: <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> Acesso em jun. 2023.

BRIGNULL, Harry. **Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You**. Londres: Testimonium Ltd, 2023.

BÜCHI, Moritz *et al*. **The chilling effects of algorithmic profiling: Mapping the issues**. Computer Law and Security Review, v. 36, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919303784> Acesso em ago. 2023.

CALIFORNIA LEGISLATIVE INFORMATION. **Civil Code – CIV. Title 1.81.5. California Consumer Privacy Act of 2018**. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> Acesso em set. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 21-A de 2020. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil; e dá outras providências**. Brasília, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9063365&ts=1679601923682&disposition=inline&_gl=1*ejnfbr*_ga*NTQ1OTIzNzcyLjE2NTE3Njg0NDk.*_ga_CW3ZH25XMK*MTY4NTk4NjEzNy4yLjAuMTY4NTk4NjEzNy4wLjAuMA..> Acesso em mar. 2023.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional**. – 6. ed. rev. Coimbra: Livraria Almedina, 1993.

CARA, Corina. **Dark Patterns in the Media: A Systematic Review**. Network Intelligence Studies, v. VII, n. 14, p. 105–113, 2019. Disponível em:

<https://www.semanticscholar.org/paper/Dark-Patterns-In-The-Media%3A-A-Systematic-Review-Cara/54c7c604f4cd4548de4b2e2e701030276d2537f8> Acesso em jul. 2023.

CARROLL, Micah *et al*. **Characterizing Manipulation from AI Systems**. Association for Computing Machinery, 2023. v. 1. Disponível em: <https://arxiv.org/pdf/2303.09387.pdf> Acesso em set. 2023.

CLARKE, Roger. **Why the world wants controls over Artificial Intelligence**. Computer Law and Security Review, v. 35, n. 4, p. 423–433, 2019. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919301268> Acesso em mar. 2023.

COELHO, Helder. **Inteligência Artificial em 25 lições**. Fundação Calouste Gulbenkian, 1995.

CONTI, Gregory; SOBIESK, Edward. **Malicious Interface Design: Exploiting the User**. Raleigh: Proceedings of the 19th International Conference on World Wide Web – WWW'10, 2010, p. 271-280. Disponível em: <https://dl.acm.org/doi/10.1145/1772690.1772719> Acesso em jun. 2023.

CORREIA, Pedro; GARCIA, Bruno C. **Inteligência Artificial e Políticas Públicas**. In: PEDRO, Ricardo; CALIENDO, Paulo. Inteligência Artificial no Contexto do Direito Público: Portugal e Brasil. Coimbra: Almedina, 2023.

DE GREGORIO, Giovanni. **Democratising online content moderation: A constitutional framework**. Computer Law and Security Review, v. 36, p. 105374, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364919303851> Acesso em mai. 2023.

DECEPTIVE PATTERNS. **Forced action**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/forced-action> Acesso em jul. 2023.

DECEPTIVE PATTERNS. **Hard to cancel**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/hard-to-cancel> Acesso em jul. 2023.

DECEPTIVE PATTERNS. **Nagging**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/nagging > Acesso em jul. 2023.

DECEPTIVE PATTERNS. **Preselection**. Types of deceptive pattern. Disponível em: <https://www.deceptive.design/types/preselection> Acesso em jul. 2023.

DI GERONIMO, Linda *et al*. **UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception**. Conference on Human Factors in Computing Systems - Proceedings, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> Acesso em jun. 2023.

DIÁRIO OFICIAL DA UNIÃO. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados. ed. 39., seção 1, p. 59. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf> Acesso em set. 2023.

DICIONÁRIO DA LÍNGUA PORTUGUESA**. "Manipulação" no Dicionário da Língua Portuguesa**. Academia das Ciências de Lisboa. Disponível em https://dicionario.acad-ciencias.pt/pesquisa/?word=manipulação> Acesso em jun. 2023.

EG, Ragnhild; DEMIRKOL TØNNESEN, Özlem Demirko; TENNFJORD, Merete Kolberg. **A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors**. Computers in Human Behavior Reports, v. 9, n. November 2022, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2451958822000872?via%3Dihub> Acesso em ago. 2023.

EUROPEAN COMISSION. **High-Level Expert Group on Artificial Intelligence**. Brussels, 2022. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> Acesso em mar. 2023.

EUROPEAN COMISSION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts**. Brussels, 2021. Disponível em: <eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206> Acesso em mar. 2023.

EUROPEAN COMISSION. **White Paper on Artificial Intelligence – A European approach to excellence and trust**. Brussels, 2020. Disponível em: <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf> Acesso em mai. 2023.

EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, LUPIÁÑEZ-VILLANUEVA, FRANCISCO ET AL. **Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report**. Publications Office of the European Union, 2022. Disponível em: <https://data.europa.eu/doi/10.2838/859030> Acesso em jun. 2022.

EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them**. Version 2.0. February, p. 1–74, 2023. Disponível em: <https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf> Acesso em set. 2023.

EUROPEAN PARLIAMENT. **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf> Acesso em set. 2023.

EUROPEAN PARLIAMENT. **Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union**

Legislative Acts (COM (2021) 0206 – C9 0146/2021 – 2021/0106 (COD)). 2023. Disponível em: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf> Acesso em jun. 2023.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Official Journal of the European Union. Brussels, 2016. Disponível em: <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)> Acesso em ago. 2023.

EUROPEAN PARLIAMENT. **MEPs ready to negotiate first-ever rules for safe and transparent AI**. News, 14 jun. 2023. Disponível em: <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai> Acesso em set. 2023.

EUROPEAN UNION. **Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925> Acesso em set. 2023.

EUROPEAN UNION. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014> Acesso em jun. 2023.

FEDERAL TRADE COMMISSION. **Bringing Dark Patterns to Light**. USA, 2022. Disponível em: <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800 Dark Patterns Report 9.14.2022 - FINAL.pdf> Acesso em jun. 2023.

FEDERAL TRADE COMMISSION. **Federal Trade Commission Act incorporating U.S. SAFE WEB Act Amendments of 2006**. Disponível em: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim> Acesso em jun. 2023.

FERRARIS, Valeria; BOSCO, Francesca; D'ANGELO, Elena. **The Impact of Profiling on Fundamental Rights**. SSRN Electronic Journal, p. 1–45, 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753> Acesso em ago. 2023.

FRANKISH, Keith; RAMSEY, William M. **The Cambridge Handbook of Artificial Intelligence**. Cambridge: Cambridge University Press, 2014. Disponível em: <https://www.cambridge.org/core/books/the-cambridge-handbook-of-artificial-intelligence/3DCB2E04739722A99EDE86B7A34A30E3> Acesso em mai. 2023.

FRANKLIN, Matija; TOMEI, Philip; GORMAN, Rebecca. **Vague concepts in the EU Ai Act will not protect citizens from AI manipulation**. OECD.AI Policy Observatory, 2023.

Disponível em: <https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions> Acesso em set. 2023.

FITZPATRICK, Noel; KELLEHER, John D. **On the Exactitude of Big Data: La Bêtise and Artificial Intelligence**. La Deluziana, 2018. doi: 10.21427/dfw8-m918. Disponível em: <https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1005&context=gradcamart> Acesso em jun. 2023.

FLORIDI, Luciano. **Information: A Very Short Introduction**. New York: Oxford University Press, 2010.

FOGG, Brian Jeffrey. **Persuasive technology**. Ubiquity, v. 2002, n. December, p. 2, 2002. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/764008.763957> Acesso em jun. 2023.

GASSER, Urs; ALMEIDA, Virgilio A.F. **A Layered Model for AI Governance**. IEEE Internet Computing, vol. 21, 2017, 58–62. Disponível em: <https://dash.harvard.edu/handle/1/34390353> Acesso em ago. 2022.

GENERAL ASSEMBLY OF THE STATE OF COLORADO. **Colorado Privacy Act**. Senate Bill 21-190, 2021. Disponível em: <https://legiscan.com/CO/text/SB190/2021> Acesso em set. 2023.

GRAY, Colin M. *et al*. **The dark (patterns) side of UX design**. Conference on Human Factors in Computing Systems - Proceedings, v. 2018- April, p. 1–14, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> Acesso em jul. 2023.

GRUDIN, Jonathan. **AI and HCI: Two Fields Divided by a Common Focus**. AI Magazine, *[S. l.]*, v. 30, n. 4, p. 48, 2009. DOI: 10.1609/aimag.v30i4.2271. Disponível em: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2271> Acesso em abr. 2023.

GUNAWAN, Johanna *et al*. **A Comparative Study of Dark Patterns across Web and Mobile Modalities**. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. CSCW2, 2021. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3479521> Acesso em jun. 2023.

HAENLEIN, Michael; KAPLAN, Andreas. **A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence**. California: California Management Review, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0008125619864925?casa_token=zVeExM_jERMAAAAA:LFj7BHbmorHWyYWpZmDm5DcTSJL900kV450sAMUa7UsC821NRBVD-P7OxkK_F3H1SdWd3SLVDEjtLA> Acesso em jan. 2023.

HARRIS, Tristan. **The Slot Machine in your Pocket**. Spiegel International, 2016. Disponível em: <https://www.spiegel.de/international/zeitgeist/smartphone-addiction-is-part-of-the-design-a-1104237.html> Acesso em jul. 2023.

HAWKING, Stephen. **Comments: The Ethics of Artificial Intelligence**. In: BATTRO, Antonio M.; DEHAENE, Stanislas. Power and Limits of Artificial Intelligence. Vatican City: Libreria Editrice Vaticana, 2017. Disponível em:

<https://www.pas.va/content/dam/casinapioiv/pas/pdf-volumi/scripta-varia/sv132pas.pdf> Acesso em mai. 2023.

HIDALGO, César A. **How Humans judge Machines**. Cambridge, Massachusetts: The MIT Press, 2021.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital: desafios para o direito**. – 2. ed. – Rio de Janeiro: Forense, 2022.

IDISIS, Gil'ad. **How to Make Lemonade from Lemons: Achieving Better Free Speech Protection Without Altering the Existing Legal Protection for Censorship in Cyberspace**. Campbell Law Review, v. 36, 2014. Disponível em: <https://scholarship.law.campbell.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1576&context=clr> Acesso em mai. 2023. p. 152.

JOHNSON, Eric J. *et al*. **Beyond nudges: Tools of a choice architecture**. Marketing Letters, v. 23, n. 2, p. 487–504, 2012. Disponível em: <https://link.springer.com/article/10.1007/s11002-012-9186-1> Acesso em jun. 2023.

KLONICK, Kate. **The New Governors: The People, Rules, and Processes Governing Online Speech**. Harvard Law Review, 2018. Vol. 131. Disponível em: <https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf> Acesso em mai. 2023.

KPMG. **The shape of AI Governance to come**. KPMG International, 2021. Disponível em: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2021/01/the-shape-of-ai-governance-to-come.pdf> Acesso em set. 2023.

LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial: entre categorias e conceitos, a busca por marcos regulatórios**. – Indaiatuba, SP: Foco, 2022.

LANIER, Jaron. **Ten Arguments for Deleting your Social Media Accounts Right Now**. 1. ed. New York: Henry Holt and Company, 2018.

LARSSON, Stefan. **On the Governance of Artificial Intelligence through Ethics Guidelines**. Asian Journal of Law and Society, v. 7, n. 3, p. 437–451, 2020. Disponível em: <https://www.cambridge.org/core/journals/asian-journal-of-law-and-society/article/on-the-governance-of-artificial-intelligence-through-ethics-guidelines/992BD33CA7CBBE83E2FBBF6B0179896C> Acesso em ago. 2022

LEE, Kai-fu. **Inteligência artificial: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos**. Trad. de Marcelo Barbão. 1. ed. – Rio de Janeiro: Globo Livros, 2019.

LEE, Kai-fu. QIUFAN, Chen. **Inteligência Artificial 2041: Dez Visões para o Nosso Futuro**. Trad. de Maria do Carmo Figueira. Lisboa: Relógio D'Água, 2023.

LYNCH, Shana. **Andrew Ng: Why AI is the New Electricity**. Insights by Stanford Business, 2017. Disponível em: <https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity> Acesso em mar. 2023.

MAGRANI, Eduardo. **A internet das coisas**. – Rio de Janeiro: FGV Editora, 2018.

MAIER, Maximilian; HARR, Rikard. **Dark design patterns: An end-user perspective**. Human Technology, v. 16, n. 2, p. 170–199, 2020. Disponível em: <https://ht.csr-pub.eu/index.php/ht/article/view/6> Acesso em jun. 2023.

MATHUR, Arunesh *et al*. **What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods**. Conference on Human Factors in Computing Systems - Proceedings, 2021. Disponível em: <https://doi.org/10.48550/arXiv.2101.04843>
Acesso em jun. 2023.

MERRIT, Kamarin; ZHAO, Shichao. **An Innovative Reflection Based on Critically Applying UX Design Principles**. Journal of Open Innovation: Technology, Market, and Complexity. 2021, 7, 129. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2199853122008988> Acesso em jun. 2023.

MICHAELS, Jordyn. **Pathways to the Light: Realistic Tactics to Address Dark Patterns**. Rutgers Computer & Technology Law Journal, vol. 49, Nbr. 1, March 2023. Disponível em: <https://law-journals-books.vlex.com/vid/pathways-to-the-light-921006230> Acesso em jul. 2023.

MILLER, Katharine. **Can't Unsubscribe? Blame Dark Patterns**. Stanford University. Human-Centered Artificial Intelligence, 2021. Disponível em: <https://hai.stanford.edu/news/cant-unsubscribe-blame-dark-patterns> Acesso em jul. 2023.

MINSKY, Marvin. **Steps Toward Artificial Intelligence**. IRE, 1960. Disponível em: <https://web.media.mit.edu/~minsky/papers/steps.html> Acesso em mar. 2023.

MOOR, James. **The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years**. AI Magazine, vol. 27, n. 4, 2006. Disponível em: <https://aaai.org/ojs/index.php/aimagazine/article/view/1911/1809> Acesso em mar. 2023.

MORAES, Alexandre de. **Direito Constitucional**. – 33. ed. rev. e atual. até a EC n. 95 de 15 de dezembro de 2016. – São Paulo: Atlas, 2017.

NARAYANAN, Arvind. *et al*. **Dark Patterns: Past, Present, and Future - The Evolution of Tricky User Interfaces**. ACM Queue, v. 18, n. 2, p. 67–92, 2020. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3400899.3400901> Acesso em jun. 2023.

NELISSEN, Lei; FUNK, Mathias. **Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments**. International Journal of Design, v. 16, n. 1, p. 75–92, 2022. Disponível em: <http://www.ijdesign.org/index.php/IJDesign/article/view/4117> Acesso em jul. 2023.

NEWMAN, Stephen J.; DENSON, Allen H.; MA, Jimmy L. **Potential First Amendment Defenses to a Dark Patterns Claim**. Intellectual Property & Technology Law Journal, v. 35,

n. 4, 2022. Disponível em: <https://www.stroock.com/uploads/Newman-Denson-Ma-copy1.pdf> Acesso em jul. 2023.

NEUWIRTH, Rostam J. **Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)**. Computer Law and Security Review, v. 48, p. 105798, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000092> Acesso em ago. 2023.

NIELSEN, Jakob. **10 Usability Heuristics for User Interface Design**. Nielsen Norman Group, 2020. Disponível em: <https://www.nngroup.com/articles/ten-usability-heuristics/> Acesso em jun. 2023.

NIELSEN, Jakob; MOLICH, Rolf. **Heuristic evaluation of user interfaces**. Conference on Human Factors in Computing Systems - Proceedings, n. April, p. 249–256, 1990. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/97243.97281> Acesso em jun. 2023.

NILSSON, Nils J. **Artificial Intelligence: A New Synthesis**. Morgan Kaufmann Publishers, 1998.

NILSSON, Nils J. **The Quest for Artificial Intelligence: a history of ideas and achievements**. Cambridge University Press, 2010.

NOVELINO, Marcelo. **Curso de Direito Constitucional**. – 11. ed. rev., ampl. e atual. – Salvador: Editora Juspodivm, 2016.

OECD. **Dark Commercial Patterns**. OECD Digital Economy Papers, n. 336. Paris: OECD Publishing, 2022. Disponível em: <https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1689002228&id=id&accname=guest&checksum=81CF1B543AA5553A7A0B0C8D1F000A6A> Acesso em jun. 2023.

OECD. **Recommendation of the Council on Artificial Intelligence**. Paris: OECD, 2019. Disponível em: <https://www.oecd.org/digital/artificial-intelligence/> Acesso em nov. 2022.

OFFICIAL JOURNAL OF THE EUROPEAN UNION. **Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2016/C 202/01)**, 2007. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT> Acesso em mai. 2023.

ÖZDEMIR, Şebnem. **Digital nudges and dark patterns: The angels and the archfiends of digital communication**. Digital Scholarship in the Humanities, v. 35, n. 2, p. 417–428, 2020. Disponível em: <https://academic.oup.com/dsh/article-abstract/35/2/417/5372748?redirectedFrom=fulltext> Acesso em jul. 2023.

PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You**. New York: The Penguim Press, 2011.

PEI, Huining *et al*. **A personalized recommendation method under the cloud platform based on users' long-term preferences and instant interests**. Advanced Engineering Informatics, v. 54, n. May, p. 101763, 2022. Disponível em: < A personalized recommendation

method under the cloud platform based on users' long-term preferences and instant interests - ScienceDirect> Acesso em ago. 2023.

PESSIS-PASTERNAK, Guitta. **Será Preciso Queimar Descartes? Do caos à inteligência artificial: quando os cientistas se interrogam**. Trad. de Manuel Alberto. – Lisboa: Relógio D'Água, 1993.

PORTO EDITORA. **"Manipulação" no Dicionário infopédia da Língua Portuguesa** [em linha]. Porto: Porto Editora. Disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/manipulação> Acesso em jun. 2023.

PRIVACY INTERNATIONAL; ARTICLE 19. **Privacy and Freedom of Expression in the Age of Artificial Intelligence**. April, 2018. Disponível em: <https://privacyinternational.org/sites/default/files/2018-04/Privacy and Freedom of Expression In the Age of Artificial Intelligence.pdf> Acesso em ago. 2023.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 4. ed., 2022.

SANTORO, Erik; MONIN, Benoît. **The AI Effect: People rate distinctively human attributes as more essential to being human after learning about artificial intelligence advances**. Journal of Experimental Social Psychology, vol. 107, n. 104464, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0022103123000215?pes=vor> Acesso em mai. 2023.

SAURA, José Ramón; PALACIOS-MARQUÉS, Daniel; ITURRICHA-FERNÁNDEZ, Agustín. **Ethical design in social media: Assessing the main performance measurements of user online behavior modification**. Journal of Business Research, v. 129, n. March, p. 271–281, 2021. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0148296321001545> Acesso em jun. 2023.

SENADO FEDERAL. **Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado n. 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei n. 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Brasília, 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9221643&ts=1671480646036&disposition=inline> Acesso em mar. 2023.

SENATE OF THE UNITED STATES OF AMERICA. **S. 1084, Deceptive Experiences to Online Users Reduction Act**, 2021. Disponível em: <https://www.congress.gov/116/bills/s1084/BILLS-116s1084is.pdf> Acesso em set. 2023.

SENATE OF THE UNITED STATES OF AMERICA. **S. 1356**, **Assuring Safe, Secure, and Ethical Systems for AI Act,** 2023. Disponível em: <https://www.congress.gov/bill/118th-congress/senate-bill/1356/text> Acesso em set. 2023.

SHWAB, Klaus. **The Fourth Industrial Revolution**. World Economic Forum, 2016.

SHIRAI, Yoshiaki; TSUJII, Jun-ichi. **Inteligência Artificial: conceitos, técnicas e aplicações**. Trad. de António Realinho. Publicações Europa América, 1988.

SIMON, Herbert A. **Artificial intelligence: an empirical science**. Artificial Intelligence, v. 77, n. 1, p. 95–127, 1995. Disponível em: <https://www.sciencedirect.com/science/article/pii/000437029500039H?ref=cra_js_challenge&fr=RR-1> Acesso em jan. 2023.

SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. New York University Press, 2004.

THE WHITE HOUSE. **Maintaining American Leadership in Artificial Intelligence**. Executive Order n. 13.859, of February 11, 2019. Disponível em: <https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf> Acesso em set. 2023.

THE WHITE HOUSE. **National Artificial Intelligence Initiative Office (NAIIO)**. Division E, Title LI, Section 5102, 2021. Disponível em: <https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf - page=1213> Acesso em set. 2023.

TJOSTHEIM, Ingvar *et al*. **Dark Pattern: A Serious Game for Learning About the Dangers of Sharing Data**. Proceedings of the European Conference on Games-based Learning, v. 2022-October, p. 774–783, 2022. Disponível em: <https://nla.brage.unit.no/nla-xmlui/handle/11250/3025227> Acesso em jul. 2023.

T.K., Balaji; ANNAVARAPU, Chandra S. R.; BABLANI, Annushree. **Machine learning algorithms for social media analysis: A survey**. Computer Science Review, v. 40, p. 100395, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013721000356> Acesso em ago. 2023.

UTZ, C. *et al*. **(Un)informed Consent: Studying GDPR consent notices in the field**. Proceedings of the ACM Conference on Computer and Communications Security, p. 973–990, 2019. Disponível em: <https://arxiv.org/pdf/1909.02638.pdf> Acesso em jun. 2023.

VARELA, Bartolomeu. **Elementos de Estudo da Teoria da Constituição**. Praia: Universidade de Cabo Verde, 2011.

VILLANI, Cédric. **Artificial Intelligence – Big Achievements and Huge Questions Viewed from Mathematics**. In: BATTRO, Antonio M.; DEHAENE, Stanislas. Power and Limits of Artificial Intelligence. Vatican City: Libreria Editrice Vaticana, 2017. Disponível em: <https://www.pas.va/content/dam/casinapioiv/pas/pdf-volumi/scripta-varia/sv132pas.pdf> Acesso em ago. 2023.

WANG, Pei. **What Do You Mean by "AI"?** Frontiers in Artificial Intelligence and Applications, vol. 171, 362-373, 2008. Disponível em: <https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf> Acesso em mai. 2023.

WEINMANN, Markus; SCHNEIDER, Christoph; BROCKE, Jan vom. **Digital Nudging**. Business and Information Systems Engineering, v. 58, n. 6, p. 433–436, 2016. Disponível em: <https://link.springer.com/content/pdf/10.1007/s12599-016-0453-1.pdf> Acesso em jun. 2023.

WE ARE SOCIAL. **The Global State of Digital in October 2022**, 2022. Disponível em: <https://wearesocial.com/us/blog/2022/10/the-global-state-of-digital-in-october-2022/> Acesso em ago. 2023.

YEUNG, Karen. **Algorithmic Regulation: A Critical Interrogation**. King's College London Dickson Poon School of Law. Legal Studies Research Paper Series. n. 2017-27, p. 1–45, 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505> Acesso em ago. 2023.

YU, Ronald; ALÌ, Gabriele Spina. **What's Inside the Black Box? AI Challenges for Lawyers and Researchers**. Legal Information Management, v. 19, n. 01, p. 2–13, 2019. Disponível em: <https://www.cambridge.org/core/journals/legal-information-management/article/whats-inside-the-black-box-ai-challenges-for-lawyers-and-researchers/8A547878999427F7222C3CEFC3CE5E01> Acesso em ago. 2023.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Public Affairs: Nova Iorque, 2019. ISBN 978-1-61039-570-0.